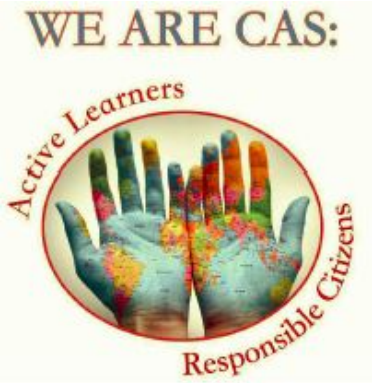
UNDERSTANDING
EXCELLENCE
&
KNOWLEDGE

CASABLANCA AMERICAN SCHOOL

Technology at CAS

- Staff

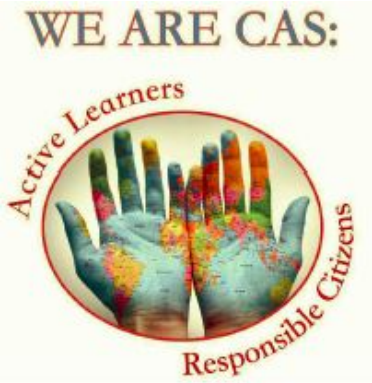


Internet Access and Security

At Casablanca American School, all faculty staff are given a school issued device to use during the year. Staff use a combination of Mac's, PC's, IPads and Chromebooks. Each classroom also has a dedicated desktop computer.

All staff devices are set to automatically connect to the staff network after first login. Staff can also connect personal devices such as smartphones to the staff network using the same credentials. Students connect to the student network only. Students do not have, or should never be given access to staff or guest networks. In cases where students and staff need to be connected to the same network, for example, if using a specific app together, staff can request access to a dedicated wifi network from IT Office.

Our network traffic is filtered through a firewall. Our filters are set up to protect users. Filtering is more restrictive on the student and guest networks. Teachers should ensure that student are not using their cell phones as hotspots. Using these allows students to circumvent network restrictions.



Your Device

Collecting your Device

At the beginning of the school year you will collect your device from the IT Office located on the 2nd floor of the lower school building. The IT Office will issue your login details. The office can be reached by dialing ext. 184.

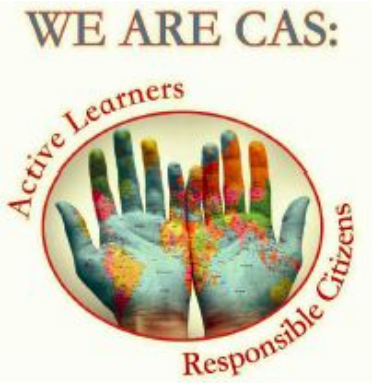
Using your Device

You should exercise care to ensure that your device functions at its fullest capacity. Some useful tips:

- Avoid leaving your device in hot areas for long periods, including direct sunlight and hot appliances as heat can damage the capacity of the battery.
- At least once a month complete a charge cycle. This means using all of your battery's power, then recharging it fully.
- Do a complete shutdown regularly. This means closing down all applications and shutting down the device. Security is paramount and this will ensure that all patches and updates are applied to your system.
- Please ensure you always care for and protect your school provided device to avoid damage or loss. Staff may be held responsible for any negligence at the discretion of the IT Director and administration.

Protecting your Data

We are a G-Suites school. G-Suites is a brand of cloud computing developed by Google that includes apps such as Gmail, Drive, Calendar and Docs. These apps improve productivity and collaboration. Given their ability to streamline workflow staff should be mindful of security when using these apps. Below are several guidelines which should be adhered to when using these apps and using devices to access these.



Passwords

You will have one password to login to the google cloud. Some **guidelines** for creating passwords and looking after passwords are:

- Between 8-12 characters.
- Mix upper case, lower case, numbers and special characters to strengthen this.
- Use 2 step verification
  2 step verification is a Google feature that requires 2 layers of security. Logging into your email requires the usual login password, additionally a code is sent to the users mobile phone to confirm identity. This can be set up in your Google account.
- Do not share passwords with anyone or store passwords unencrypted.

Browsers

Your browser includes additional functionality to help improve your browsing experience. We recommend modifying some of these features to help protect yourself and your data.

- **Saving passwords:** You can save site passwords in your browser to save you having to remember them at next login. Do not save passwords for sites that contain personal or sensitive student data. Saved browser passwords are vulnerable and are easy to decrypt.
- **Syncing data**: Choosing to sync items in your bowser like history and bookmarks means that when you sign into the browser on another device you will have access these. Student Information Systems and other data sensitive applications should not be synced. You can tailor what is synced to in the sync settings. Do not sync passwords. Additionally, you can add a passphrase in google Chrome that will add a second layer of security.

Screen Lock

As part of our security measures all desktop computers in classrooms will automatically lock after 20 minutes of inactivity. You have control over this on your own device but

you should ensure that you have this feature enabled and manually lock your device if you are leaving it unattended.

Sharing Devices

Staff are assigned their own device so they can safely and securely access their own data and the school network. You should not share your device with anyone.

Communication in CAS

Like all institutions, at CAS, appropriate communication is vital to success. Effective Communication with all stakeholders plays a vital role in achieving the goals of our vision statement. With this in mind, the following guidelines should be adhered to when communicating with stakeholders:

Parents

- Primarily, the student information system should be used for mass parent communication. Where the recipients of the communication are few school email can be used. Do not use email groups nor cc' functions with communications to parents.

Students

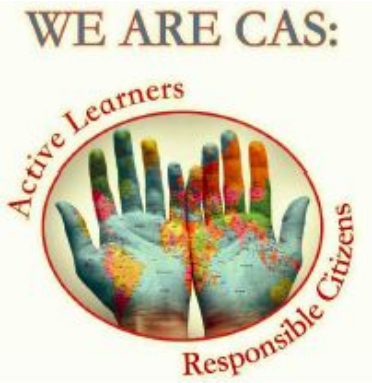
- School email should be used to communicate with individual students. Grade level or school wide communications should always be sent through Renweb and or Managebac.

Staff

- School email should be used to communicate internally with CAS staff.

External Communities

- School email should always be used in communications with any external agencies.



US and LS Principals may also direct staff on methods of communication appropriate to their respective schools.

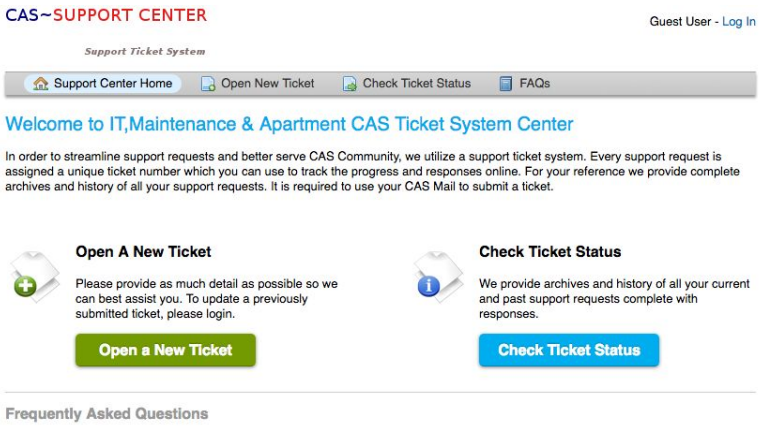
Considerations when Sending Email

- Subject line should clearly communicate the purpose of the email. Never identify a student in a subject header.
- Keep an email concise and to the point.
- Never use Reply All when a Reply is sufficient.
    - To avoid chain communications use bcc, notify recipients that you are doing so, not to hide who you are sending to, rather to avoid chain responses.
- Do not forward chain-letters or irrelevant messages to the CAS community.
- Do not engage in personal chat with students via email.
- Add an email signature to your email.

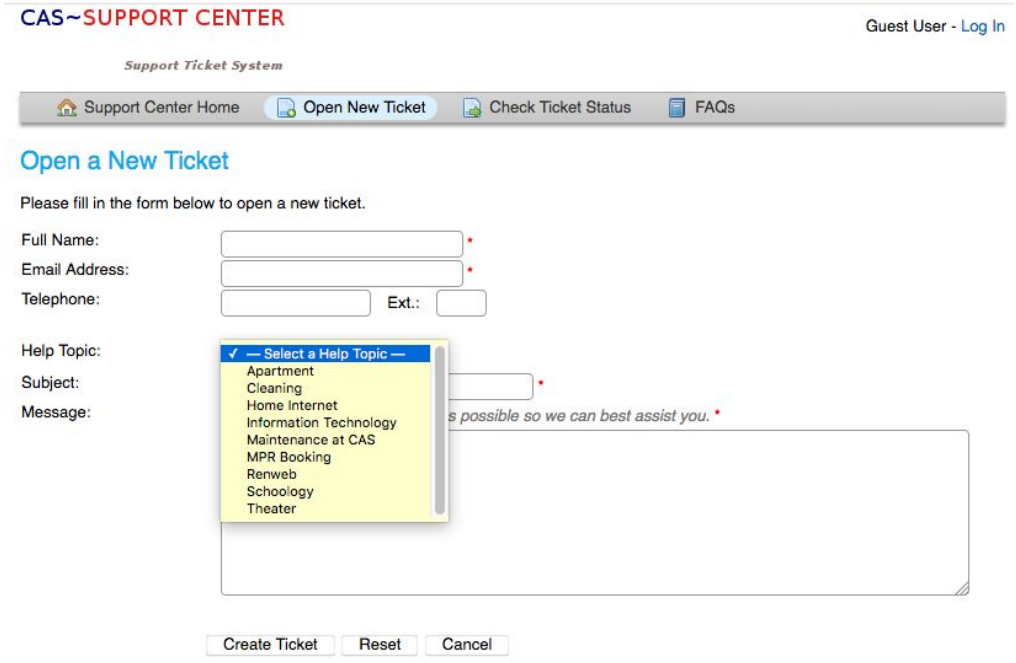
Support at CAS

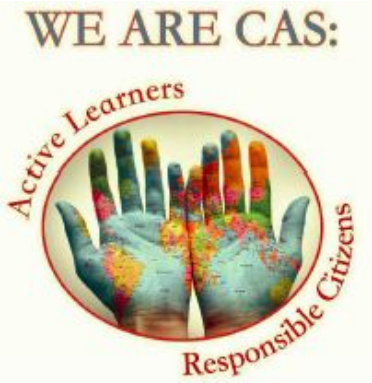
We operate an online ticket system for IT support, other support requests such as maintenance in school and apartment maintenance and booking rooms. You can open a ticket through the following link http://helpdesk.cas.ac.ma/helpdesk/ and follow these steps:

1. Click on *open a ticket*.



2. Fill in the form details and choose the area you require assistance with, adding as much detail to the message portion as you can regarding your issue.

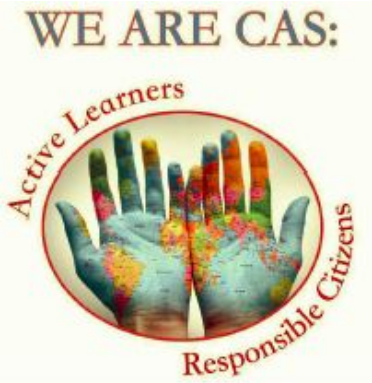




You will receive a timely response from the department designated to deal with the topic area. The IT department cover Renweb, Schoology and Information Technology.

In the event of an emergency you can also locate support from the IT office on the second floor of the lower school building or from the Tech Directors office on the ground floor of the US building. Telephone extensions are:

196 - Mags
184 - Nabil, Mohammed, Adil



Acceptable Use

Staff being connected to the global community brings both opportunities and responsibilities. In general, staff are expected to communicate in a professional manner consistent with CAS vision and mission statements, inline with Moroccan law governing the behavior of school employees and with international laws governing copyrights.

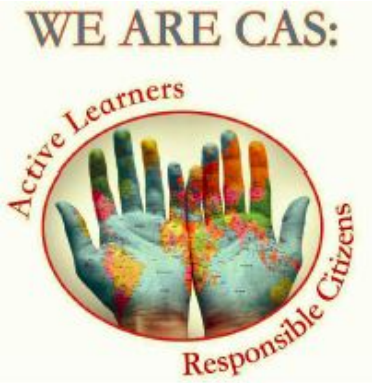
The network is provided for staff to conduct research, communicate with others and augment and enhance the efficiency as well as the overall performance of the staff members duties.

Communications over the network are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The employee shall be accountable to his/her immediate supervisor in the use of technology.

The following behaviours are strictly prohibited:

1. Using communication media to share confidential information about students or other employees.
2. Providing anyone with legally restricted or confidential information on students or employees.
3. Sending or displaying offensive messages or images.
4. Assisting a campaign for election of any person(s) to any official role or for the promotion of or opposition to any ballot proposition.
5. Using obscene or offensive language harassing, insulting or attacking others or otherwise communicating in a manner that violates Board Policy or the image and reputation of the school or any member of the school community.
6. Engaging in practices that threaten the security of the network (e.g., loading files that may introduce a virus; unauthorized downloading of programs or installing any software, not properly safeguarding information such as passwords).
7. Violating copyright laws.



8. Trying to obtain or using others' passwords.
9. Trespassing in others' personal devices or files.
10. Employing the network for commercial purposes.
11. Day trading or gambling.
12. Circumventing the filtering policy by connecting personal electronics through wireless access or other data networks not authorized for use by the CAS IT department.

I have read understood and hereby agree to comply with the Acceptable Use Policy at Casablanca American School.

_____

Staff Name

_____ _____

Staff Signature Date