INFORMATION & COMMUNICATION TECHNOLOGY (ICT)

ACCEPTABLE USE POLICY (AUP) – STUDENTS

Policy Status | CURRENT
---|---
Policy Classification | Board Endorsed
Policy Established | 2005
Policy Last Reviewed | 2014
Policy Responsibility | Student Services Office/Deans

Policy, Forms, and Agreements

St Augustine’s College offers ICT (Internet, email, computer equipment, network resources) access for student use. The following documents contain the student ICT policy, forms, and agreements to implement the College ICT Acceptable Use Policy. This policy operates in conjunction with the College’s Social Networking and Social Media Policy.

A. Educational Purpose

1. As we educate our students for a rapidly changing world, we believe it is important for them to learn how to use technology constructively and responsibly.

2. The College ICT system is limited to educational purposes which include the use of the system for learning activities including suitable research.

3. The College ICT system must not be used for commercial purposes such as offering, providing or purchase products or services through the system.

B. Student Access to the College ICT system

1. All students are issued with an individual network account.

2. All students must sign an Account Agreement to be granted an individual account on the College ICT system. Parents can withdraw their approval at any time.

C. Unacceptable Uses

The following uses of the College ICT system are considered unacceptable whether carried out on a College-provided or personally owned device:
1. Personal Safety
   (a) Posting personal contact information about yourself or other people including (but not limited to) addresses, telephone numbers, email addresses etc.
   (b) Agreeing to meet with someone you have met online without parental approval. Students must promptly disclose (to a teacher or other school employee) any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal or Inappropriate Activities
   (a) Using College-issued or personal devices to cheat on assignments, quizzes, or tests.
   (b) Using College-issues of personal devices for non-educational purposes (such as making personal phone calls and text messaging) without the permission of a staff member.
   (c) Attempting to gain unauthorized access to the College network or any other computer system through the College network or go beyond your authorized access. This includes attempting to log in through another person's account or access or interfere with another person's files. These actions are illegal, even if only for the purposes of "browsing".
   (d) Students are responsible for their own individual account and should take all reasonable precautions to prevent others from being able to access it. After each use you should log out of the system. Under no conditions should you provide your password to another person.
   (e) Students should immediately notify a teacher or IT Manager if they have identified a possible security problem. Students must not go looking for security problems, as this may be construed as an illegal attempt to gain access.
   (f) Using a device to make deliberate attempts to infect the College network or any other computer system with a virus, Trojan or programme designed to damage, alter, destroy or provide access to unauthorised data or information. These actions are illegal.
   (g) Using the College system to engage in any other illegal activity.

3. Inappropriate Language and Personal Attacks
   (a) Posting material on any web page, social media, smart phone or public or private messages using inappropriate language. This includes using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
   (b) Posting information that could cause damage or a danger of disruption.
   (c) Engaging in personal attacks, including prejudicial or discriminatory attacks.
   (d) Harassing another person. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by a person to stop sending them messages, you must stop.
   (e) Posting false or defamatory information about a person or organization.
   (f) Further details can be found in the College’s Social Networking and Social Media Policy
4. Respect for Privacy
   (a) Using devices to record, transmit, post or purposefully access photographic images or video on College premises during school hours or during school activities without permission provided by an appropriate member of staff.
   (b) Reposting a message that was sent to you privately without permission of the person who sent you the message.
   (c) Posting private information about another person.
   (d) Further details can be found in the College's Social Networking and Social Media Policy

5. Respecting Resource Limits.
   (a) Downloading large files unless absolutely necessary. If necessary, permission must be first sought from a member of the IT Department.
   (b) Posting chain-letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

6. Copyright Infringement
   (a) Failing to respect the rights of copyright owners. Copyright infringement occurs when work that is protected by copyright is inappropriately reproduced. If a work contains language that specifies appropriate use of that work, these requirements must be followed. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be very confusing: If you have questions ask a teacher.

7. Access to Inappropriate Material
   (a) Attempting to bypass the College’s web filters.
   (b) Using the College system to access material that is profane or obscene (pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (hate literature). A special exception may be made if the purpose of your access is to conduct research under your teacher’s guidance.
      Inappropriate material accidentally accessed should immediately be reported to a teacher or the College IT Manager. This will protect you against a claim that you have intentionally violated this policy.
   (c) Students are bound by any additional guidelines regarding inappropriate material set by their parents.

8. College Provided ICT Equipment
   (a) Doing anything likely to cause damage to any equipment, whether deliberately or carelessly
(b) Stealing equipment
(c) Vandalising equipment (including graffiti)
(d) Eating or drinking near any College owned computer resources
(e) Any student who is found to vandalise or wilfully destroy College owned computer property will be charged the replacement cost

D. Additional Conditions of the BYOT Programme

The following conditions apply to students involved in the Bring Your Own Technology (BYOT) Programme

1. Purpose

(a) The Bring Your Own Technology (BYOT) programme provides access to Information and Communication Technology (ICT) resources and content 24/7, gives students the opportunity to take ownership of their learning and improves their media and technology literacy.

(b) Students will be expected to comply with all class and College rules while using personal devices. The use of technology is not a necessity but a privilege. When abused, privileges will be taken away.

(c) During the course of the school year, additional rules regarding the use of personal devices may be added.

2. Device Types

(a) For the purpose of this programme, the word “devices” will include privately owned: laptops, MacBooks, smart phones, IPods, IPads, tablets.

3. Guidelines

(a) Devices may only be used to access computer files on Internet and College portal sites which are relevant to the classroom curriculum.

(b) Students are responsible for maintenance and repairs of their devices.

(c) Students are responsible for saving their files and backing them up.

4. Students and Parents/Guardians acknowledge that:

(a) The College's network filters will be applied to a device’s connection to the Internet and any attempt to bypass the network filters is prohibited.

(b) Printing from all personal devices might not be possible at the College.

(c) Personal devices must be charged prior to school and run on battery power while at school. Charging of devices will not be permitted at the College.

5. Lost, Stolen, or Damaged Devices

(a) Each user is responsible for his own device and should use it responsibly and appropriately. St Augustine’s College takes no responsibility for stolen, lost, or
damaged devices, including lost or corrupted data on those devices. While College staff will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner’s policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.

(b) The College will not be held liable for any software or operating system corruption which includes, but is not limited, to the result of a spyware, adware, worms, viruses, Trojan horses, or malicious activity by another on the network.

6. Usage Charges

(a) St Augustine’s College is not responsible for any possible device charges to student accounts that might be incurred during use of the device at the College.

7. Network Considerations

(a) Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the “StA_BYOT/StA_BYODM” wireless network to access the Internet. Users are not permitted to use their own 3G or 4G network connection.

(b) A user may not connect more than two BYOT devices to the College network at any given time.

(c) All student must have some level of properly licensed anti-virus software with automatic updates installed on their devices in order to connect to the College network.

8. Managing battery life

(a) Students must ensure that their device is brought to school fully charged each morning.

(b) Students must appropriately manage their battery life such that sufficient life is maintained for learning activities throughout the day. The College is unable to provide chargers or charging stations.

9. Managing files

(a) All files must be backed up (in a location other than the device’s internal memory) and it is the responsibility of the student to ensure this is regularly and efficiently carried out.

(b) The College recommends the use of OneDrive due to its large data capacity and cloud-based interface.

10. Software

(a) Students are expected to use only legally-licenced software on their devices.

(b) The College takes no responsibility for any issues arising from illegally acquired software being used.
E. Privacy

1. Students should be aware that they have limited privacy in regards to the contents of their personal files and records of their online activity while on the College network.

2. Routine maintenance, Internet filtering or monitoring of the College ICT system may lead to discovery that you have violated this policy, the student disciplinary code, or the law.

3. St Augustine’s College is authorised to collect and examine any device that is suspected of causing technology problems, was the source of an attack or virus infection, or potentially breaching the this or any other College policy. If the device is locked or password protected the student will be required to unlock the device at the request of a College administrator.

4. Parents have the right to address any concerns and request restrictions of your individual account at any time.

F. Due Process

1. The College will cooperate fully with external authorities in any investigation related to any illegal activities conducted through the College ICT system.

2. In the event there is a claim that you have violated this or any other policy, you will be provided with an opportunity to present an explanation. Subsequent additional restrictions may be placed on your use of your Internet account.

G. Limitation of Liability

1. The College makes no guarantee that the functions or the services provided by or through the College ICT system will be error-free or without defect. The College will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The College is not responsible for the accuracy or quality of the information obtained through or stored on the system. The College will not be responsible for financial obligations arising through the unauthorized use of the system. Your parents can be held financially responsible for any harm to the system/computer equipment as a result of intentional misuse.
Student ICT Acceptable Use Agreement

Student Name __________________________ Tutor Group ___________

I have read the College's Student ICT Acceptable Use Policy. I agree to follow the rules contained in this Policy. I understand that if I violate the rules my account can be terminated and I may face other disciplinary measures.

Student Signature __________________________ Date ___________

Parent/Guardian Acceptable Use Agreement

I have read the College's Student ICT Acceptable Use Policy.

I hereby release the College, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my son’s use of, or inability to use, the College ICT system, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services. I understand that I can be held liable for damages caused by my son's intentional misuse of the system.

I will instruct my child regarding any restrictions against accessing material that are in addition to the restrictions set forth in the College Internet Use Policy. I will emphasize to my son the importance of following the rules for personal safety.

I give permission to issue an account for my son and certify that the information contained in this form is correct.

Parent/Guardian Name ___________________________________

Parent Signature __________________________ Date ___________