School ICT Policy

Ahliyyah & Mutran

Scholastic Year of 2020

Introduction

This document outlines the general policy used for mobile and handheld devices at the Ahliyyah School for Girls and the Bishop's School for boys in all of their educational levels, facilities and campuses. The document will refer to the aforementioned schools as ASG & BSA schools. This document can be disseminated to school students, staff, educators and parents.

Scope

This Policy sets out ASG & BSA Schools' guidelines on the use of ICT systems and the consequences of failure to comply with the Policy. The Policy applies to all ASG & BSA Schools employees, contractors, consultants, agents and any other persons who at any time use or have access to e-mail or the internet during the course of their employment or business dealings with the School, whether such use takes place on the School's premises or elsewhere. In respect of ASG & BSA schools' employees, the Policy forms part of each employee's contract of employment. In respect of other Users, the Policy forms part of the contractual relationship between the ASG & BSA schools and the User.

System Integrity and Support

All establishments have support systems in place to manage system changes and breakdowns. ASG & BSA have trained staff to give this support. All users will be informed of their local support arrangements. These should always be used whenever there is a need to move equipment, add additional facilities, equipment, peripherals or software. Unless it is part of their job description, users are not permitted to make any changes to the set-up of their computer and must not attempt to download or install application software from the internet or via e-mail. Users must not disconnect PCs or other ICT equipment from each other, from the mains supply or from network connection points; doing so may corrupt data stored on the system or the current work of other users. Users should always contact ICT support if there is a need to move any piece of ICT equipment for any reason.

Data Security

The computer system and its networks are provided for schools' business purposes. You should not create personal files or store personal data on the system, particularly music or video files which consume large amounts of storage space and data transmission capacity. The schools cannot guarantee that any personal data stored on its systems will be backed up, protected from unauthorized access or will be available for retrieval by its creator.

Passwords

Passwords will be required for various applications and access to systems. For system security, these passwords will be required to be changed from time to time. Passwords must have at least 8 characters, including at least one capital letter and one numeric digit. It is the responsibility of all users to ensure that personal passwords are not shared or disclosed to any other users. If any user believes that someone else knows his/her password, he/she should change it immediately. Students or staff should not share their password for any reason. There may be times, such as holidays or other periods of extended absence when it would be useful for other users to have access to data that is stored in another user's area. This should not be done by sharing passwords. Each network file server has a public folder, which all (staff) users can access. Documents which are not confidential can be stored or copied here and accessed by other users. If a user wishes to share confidential work with one or more trusted colleagues, the system

administrator can create a private shared space which only nominated people can access where confidential files may be shared.

Viruses

Viruses can be introduced into the schools' systems and networks or transmitted to a third party's system by sending and receiving e-mail and by using the Internet. The deliberate introduction of a virus is a criminal offence. Accidental introduction of viruses may, in certain circumstances, give rise to a claim against the school. All users must take all reasonable steps to ensure that no viruses are transmitted and must follow the school anti-virus procedures. Viruses may also be introduced when data is imported to the schools' systems using memory sticks and similar devices. Any user (staff or student) who imports material prepared on their personal computer equipment or other third-party system must ensure that the system used to prepare or amend the material is fully protected by a recognized anti-virus programme, which is kept fully up to-date. Privately owned equipment (laptop computers, MP3 players, digital cameras, etc.) must not come into contact with the network. Users (staff or student) must not attempt to connect any of their own personal equipment direct to network connections or to connections on School owned computers witout consulting the schools' ICT team first. This restriction applies to hard-wired connections to data sockets and connection via wireless access points where these exist.

E-mail and Internet Access

The use of e-mail and the Internet are efficient and cost-effective ways of communicating and obtaining information. If properly used, such means of communication are an invaluable educational and business tool. However, improper or inappropriate use of e-mail and the Internet can have an adverse effect on the schools' operation. Such use can also have serious legal consequences. All e-mails should carry the following corporate disclaimer:

This communication is from ASG & BSA Schools This message contains information, which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). Please note that any distribution, copying or use of this communication or the information in it without the authority of the School, is strictly prohibited. If you have received this communication in error, please notify postmaster and then delete the message & any copies of it. Any email attachment may contain viruses, whilst reasonable precaution has been taken to minimize this risk, we cannot accept liability for any damage which you sustain as a result of any viruses. You should therefore carry out your own virus checks before opening any attachment. Please keep your anti-virus software up to date as hundreds of new viruses are discovered each week.

If your emails do not carry the above disclaimers, please consult the schools' ICT team team for assistance.

Holidays and Absence

At most locations, the e-mail system includes the facility for an automatic message to be sent to correspondents when the user is away from his/her workplace. This facility is useful to advise senders that there will be a delay until they receive a response. If this facility is provided, it must be used whenever you the user is away from his/her workplace for more than one day.

Authorized Personal Use

Users (staff and students) are entitled to make reasonable personal use of e-mail and Internet facilities outside normal working hours, e.g. lunchtimes. Such use must be consistent with this policy. The schools reserves the right to discontinue this entitlement for all or some employees/students if it views the use of e-mail and Internet facilities as excessive or

inappropriate. Users are reminded that any personal use of e-mail cannot be considered private and may be subject to monitoring in accordance with this Policy. Users must make their own arrangements to save electronic or paper copies of their personal e-mails; the school does not accept any responsibility for the safe storage of personal e-mails, which may be deleted at any time.

Unauthorized Use

ASG & BSA schools' computer systems and networks, and provision of e-mail and Internet facilities, must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which:

- is illegal, obscene, pornographic, indecent, vulgar or threatening; contains unacceptable content, including but not limited to, sexually explicit messages, images, cartoons, jokes, or unwelcome propositions, or any other content which is designed to cause or likely to cause harassment or provocation of any other person or organization based on sex, sexual orientation, age, race, national origin, disability, religious or political belief;
- is defamatory, slanderous or libelous;
- deliberately introduces viruses into the e-mail or internet systems of the partnership or any other party or is designed to deliberately corrupt or destroy the data of other users;
- conflicts with ASG & BSA Schools' commercial interests;
- infringes or may infringe the intellectual property or other rights of the School or those of a third party;
- is part of a chain letter, "junk mail" or contains unsolicited commercial or advertising material;
- violates the privacy of other users;
- is in breach of the duty of confidentiality which the School owes to the pupils, students and members of staff of its School.
- disrupts the work of other users.

Users must not send e-mails, which make representations, contractual commitments, or any other form of statement concerning the schools unless they have specific authority from the schools to do so. Users must not register ASG & BSA schools' e-mail addresses on internet lists or websites inviting downloads, automated e-mail or remote access. ASG & BSA schools must do all it can to ensure that any inappropriate or unsuitable sites are blocked from the system.

Confidentiality

All schools' information exchanged by the means of e-mail is subject to confidentiality. No information gained through e-mails may be disseminated or passed to third parties for whom it was not intended by the originator of the e-mail. If an e-mail is misdirected and a user receives an e-mail which was not intended for him/her, he/she must at once notify the originator with information about the circumstances in which he/she received it. In no circumstances may such an e-mail be forwarded to another, except as part of an investigation into the causes of the misdirection. E-mails to recipients' external to the schools will carry an automatic disclaimer to protect the interests of the originator and of the schools. Internal e-mails between two staff members of ASG & BSA Schools will not carry such a disclaimer. The proper use of internal e-mails is governed by this Policy; any improper use of information contained within an internal e-mail will be considered gross misconduct.

Privacy and Monitoring

ASG & BSA schools may:

- monitor and record any e-mails which are transmitted over its computer system;

- monitor or record the use of the internet by employees/students, and the nature of material downloaded from the internet;
- monitor or record any use of computer equipment and user sessions.

for the following reasons:

- To ascertain whether the School's practices, policies and procedures (including this ICT Use Policy) have been complied with;
- To investigate or detect the unauthorized use by any employee's/student's computer system;
- To secure the effective operation of the School's computer system;
- To determine whether any communication has been made which relates to the business of the School; or
- For the purpose of preventing or detecting crime.

Any e-mails sent by employees/students may, therefore, be intercepted and monitored by the schools for any of the above reasons. Accordingly, any messages, which are sent, are not private. If a user wishes a message to be confidential, or if he/she wishes any Internet access to be confidential, he/she should not use the School's system.

Failure to comply with the Policy

Any failure on the part of an employee/student of ASG & BSA schools to comply with the Policy may result in disciplinary action being taken by the School. Depending upon the severity of the offence a breach of the Policy may be considered gross misconduct, which could result in dismissal.

Any failure to comply with the Policy on the part of a User who is not an employee may result in the immediate termination of the contractual or other relationship between that person or organization and the schools. Any unauthorized use of e-mail or the internet by a user which the schools, at its sole discretion, considers may amount to a criminal offence shall, without notice to the user concerned, be reported to the police or other relevant authority.