GHANA COLLEGE OF PHYSICIANS AND SURGEONS

I.C.T POLICY

Table of Contents

Contents

ABBREVIATIONS

GCPS – Ghana College of Physicians and Surgeons.

ICT – Information Communication Technology IT –
Information Technology

SLA – Service Level Agreement

ISO – International Organisation of Standards
LAN- Local Area Network

This Policy document should be read in relation to other Policy document of the College.

1.0. Preamble

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations. Ghana College of Physicians and Surgeons (GCPS) is not an exception. The Management of the College recognizes this fact; organizations all over the world, including GCPS are faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance. This ICT Policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of I.C .T by all GCPS Staff.

2.0. Objectives

The objectives of this Policy are to;

- ➢ Enhance information security of GCPS (systems security and data security.)
- ➢ Enhance best practices according to International Organization for standardization (ISO).
- ➢ Enhance efficient use of information systems by GCPS Staff, Fellows, Members and Residents.
- ➢ Continuous functioning of GCPS I.C.T System.
- ➢ Enhance a spirit of awareness, co-operation, trust and consideration for users.

3.0. Scope

The ICT Policy document relates to all Information Technology facilities and services provided by GCPS including, but not limited to, email system, databases, operating systems (windows and UNIX), internet, telephone systems, wireless communication, printers and copiers. All GCPS Staff, as well as Fellows, Members and Residents are expected to adhere to it. The document shall be effective from the date of approval.

4.0. Precautionary and Disciplinary Measures

Deliberate and serious breach of the Policy statements in this section will lead to disciplinary measures which may include the offender being denied access to GCPS I.C.T facilities and other sanctions as captured in the disciplinary code of the College.

4.1 Copyright:

Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

Any software or files downloaded via the Internet into the College network becomes the property of the College. Any such files or software may be used only in ways that are consistent with their licenses or copyrights and in accordance with College Policy.

Users may not upload any software licensed to the College or data owned or licensed by the College without the express authorisation of the Manager responsible for the software or data.

4.2 Security:

4.2.1 It is an offence to obtain unauthorized access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact the I.C.T Department.

4.2.2 Don't disclose personal system passwords or other security details to other staff, or external agents and don't use anyone else's login; this compromises the security of GCPS. If someone else gets to know your password, ensure you change it or get I.C.T Department to help you change.

4.2.3 If you leave your PC unattended without logging off or locking the session, you are responsible for any misuse of it while you're away.

4.2.4 Always check floppy disks and flash disks for viruses, even if you think they are clean. Computer viruses are capable of destroying GCPS information resources. It is better to be safe than sorry.

4.2.5 You are a representative of GCPS when you're on the Internet: Make sure your actions are in the interest (and spirit) of GCPS and don't leave GCPS open to legal action (e.g. libel).

4.2.6 Avoid trading insults with other people using the Internet with whom you disagree.

4.2.7 Obscenities/Pornography: Don't write it, publish it, look for it, bookmark it, access it or download it.

4.3 Electronic Espionage:

Any information available within IT facilities must not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are:

i) In the case of a specific allegation of misconduct, when the Management Team can authorise accessing of such information when investigating the allegation. This may necessitate disabling the victim from accessing IT facilities during investigation.

ii) When the IT Support Section cannot avoid accessing such information whilst fixing a problem. The person concerned will be informed immediately and information will not be disclosed .

iii) Systems administrators, database administrators and auditors in their day to day work activities.

4.4 Disciplinary Actions

A Staff found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

5.0. Email

5.1 Introduction:

GCPS makes email available to its Staff where relevant and useful for their job. This email use Policy describes the rules governing email usage at the College. It also set out how Staff are to behave when using email

5.2 Definitions

Email: messages distributed by electronic means from one computer user to one or more recipients via a network.

Email etiquette: Email etiquette refers to the principles of behaviour that one should use when writing or answering email messages.

5.3. Purpose of the Email Policy

Email is a standard way to communicate in business. It is used widely and is arguably just as important as the telephone.

Like any technology, email use can cause difficulties if it is not used correctly. This email Policy:

- ➢ Reduces the security and business risk face by GCPS.
- ➢ Enable staff know how they are permitted to use College email.
- ➢ Ensure employee follow good email etiquette
- ➢ Help the College satisfy its legal obligation regarding email use

Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. Think and check messages before sending (just as you would a letter or paper memo).

5.4 General points on email use:

5.4.1 When publishing or transmitting information externally be aware that you are representing GCPS and could be seen as speaking on GCPS's behalf. Make it clear when opinions are personal. If in doubt, consult your Line Manager.

5.4.2 Check your inbox/in-tray at regular intervals during the working day. Keep your in-tray fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

5.4.3 Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions / decisions of a colleague).

5.4.4 Don't forward emails warning about viruses (they are invariably hoaxes and systems administrators will probably already be aware of genuine viruses - if in doubt, contact them for advice). Exception: Only Systems administrators (I.C.T Personnel) can forward warnings about viruses.

5.5 Email etiquette:

5.5.1 Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are also copying another group of people.

5.5.2 Make your subject headers clear and relevant to your reader(s) e.g. don't use subject headers like "stuff" Don't send a subject header of, say "accounts" to the accountant

5.5.3 Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.

5.5.4 Capitals (eg NOW) can also be used to emphasize words, but should be used sparingly as it commonly perceived as 'shouting'.

5.5.5 Don't open email unless you have a reasonably good expectation of what it contains and the source of the mail, e.g. Do open report.doc from an Internet colleague you know, Don't open explore.zip sent from an address you've never heard of, however tempting. Alert IT Support if you are sent anything like this unsolicited. This is one of the most effective means of protecting GCPS against email virus attacks.

5.4.7 Keep email signatures short.

Your name, title, phone/fax and web site address may constitute a typical signature.

5.4.8 Understand how forwarding an email works.

If you forward mail, it appears (to the reader) to come from the originator (like passing on a sealed envelope).

If you forward mail and edit it in the process, it appears to come from you - with the originator's details usually embedded in the message. This is to show that the

original mail is no longer intact (like passing on an opened envelope).

5.6 Email security:

Used inappropriately email can be a source of security problems for the College. Users of the College's email must Not:

- ➢ Open email attachments from unknown sources, in case they contain viruses, spyware or other malwares.
- ➢ Disable security or email scanning software. These tools are essential to protect the business from security problems.
- ➢ Access another user's College email account. If they require access to specific message (while an employee is off sick), they should approach the Line Manager or the ICT department.

Staff members must always consider the security of the College systems and data when using email. If required, help and guidance is available from Line Managers and the College ICTICT Department.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception.

Although such interceptions are rare, it's best to regard email as an open communication system, not suitable for confidential messages and information.

5.7 Policy Enforcement

The College email system and software are provided for legitimate business use. The College therefore reserves the right to monitor employee use of email. Any such examination or monitoring will only be carried out by authorized staff.

Additionally all emails sent or received through the College email system is part of official College records. The College can be legally compelled to show the information to Law Enforcement agencies or other parties.

Users should always ensure that the College information sent via email is accurate, appropriate, ethical and legal.

5.7 Potential Sanctions

Knowingly breaching this Email Policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment. Staff and other users may also be held personally liable for violating this Policy.

Where appropriate the College will involve the Police or other Law Enforcement agencies in relation to breaches of this Policy.

6.0. Internet

6.1 Introduction

Access to the internet through the College is a privilege. Users granted this privilege must adhere to strict guide Lines concerning the appropriate use of this information resource. Users who violate the provisions out Lined in this document are subject to disciplinary action up to and including denial of access to this resource. In addition, any inappropriate use that involves a criminal offense will result in legal action.

6.2 Definitions

Internet: A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Local Area Network: A *local area network* (*LAN*) is a group of computers and associated devices that share a common communications Line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic *area* (for example, within an office building).

6.3. Purpose of the Internet Policy

The purpose of this internet Policy is to define the procedures for access to the internet through the College network infrastructure.

6.4 Acceptable Internet Usage

Access to the internet is specifically limited to activities in direct support of official College business.

In addition to access in support of specific work related duties, the College internet connection may be used for educational and research purposes.

This is what is defined as acceptable use within the College.

6.5 Inappropriate Internet Usage

The College internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials.

The use of College electronic mail or messaging services shall be used for the conduct of College business only. These services shall not be used to harass, intimidate or otherwise annoy another person.

The College internet access shall not be used for private, recreational, commercial, Political purposes or non-College related activity.

The use of the College internet access shall not be for personal gain such as selling access of a College user login. College Internet access shall not be used for or by performing work for profit in a manner not authorised by the College.

Users shall not attempt to circumvent or subvert security measures on the College's network resources or any other system connected to or accessible through the internet.

College Staff shall not use its internet access for interception of network traffic for any purposes unless engaged in authorised network administration.

College users shall not make or use illegal copies of copyrighted material, store such copies on College equipment or transmit these copies over the College internet.

6.6. Security

The College users who identify or perceive an actual or suspected security problem shall immediately contact the College I.C.T Department.

Users shall not reveal account password or allow another person to use their account. Similarly users shall not use the account of another user.

Access to College network resources shall be revoked for any user identified as a security risk or a demonstrated history of security problems.

6.7. Local Area Network Security and Access

Firewalls and Intrusion Detection systems shall be used across the entire GCPS network to monitor and prevent hackers, viruses and worms including all other forms of attach. The Head of ICT shall ensure that this Policy is adhered to. Failure to do this may necessitate disciplinary action depending on circumstances and top Management approval.

All computers hooked into the network shall mandatorily have an up-to-date antivirus software to prevent viruses and all other forms of malicious code. It shall be the responsibility of ICT Manager to ensure that this Policy is adhered to. Failure to which disciplinary action shall be implemented as per Management approval. All staffs are also expected to seek authority from ICT team before hooking any laptop to the network. Staffs are also expected to report timely outdated versions of antivirus for action to ICT team.

All servers shall likewise have antivirus and a form of monitoring to ensure that only authorised users have access.

6.8 Potential Sanctions

Any user violating this Policy is subject to the loss of the network privileges and any other College disciplinary actions deemed appropriate.

6.9 User Compliance

All terms and conditions as stated in this document are applicable to all users of the network and the internet connection.

7.0. Passwords

7.1 Introduction

Passwords are an important aspect of computer security and are the front Line of protection for user accounts. A poorly chosen password may result in the compromise of GCPS entire corporate network. As such, all GCPS Staff with access to systems are responsible for taking the appropriate steps, as out Lined below, to select and secure their passwords

7.2 Definitions

Password: A *password* is a string of characters that people can use to log on to a computer and access files, programmes, and other resources. Passwords help ensure that people do not access the computer unless they have been authorized to do so. It could also be define as a secret word or phrase that must be used to gain admission to a place.

Passphrase: A **passphrase** is a sequence of words or other text used to control access to a computer system, programme or data. A **passphrase** is similar to a password in usage, but is generally longer for added security. **Passphrases** are often used to control both access to, and operation of, cryptographic programmes and systems.

7.3 Purpose of the Password Policy

The purpose of this Policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

7.4 Guide Lines on Password Creation and Usage

Passwords must be changed on a regular basis according to the following schedule:

- All system-level passwords (e.g., admin, root) must be changed every 30 days.
- All user-level passwords (e.g. e-mail, Web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts that have system-level privileges granted through group memberships or programmes must have a unique password from all other accounts held by that user.

- Passwords must not be inserted into e-mail messages or other forms of electronic communication. Passwords must not be stored or transmitted in clear (unencrypted) text.
- Users are not permitted to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. Passwords/phrases shall be set by I.T Department for first time users and upon first use it shall be set to a unique one for each user and changed immediately by the user after the first use.
- All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used to restrict access to systems, software applications, and data. Some of the more common uses of passwords include user-level accounts, Web accounts, e-mail accounts, screen saver protection, voice mail passwords, and device passwords (e.g. firewalls, routers, Smartphones, Wearable Computing Devices).

When selecting a password, Staff should remember that the longer and stronger the password, the more likely it will help keep information systems, and the data contained with the systems, secure.

Where possible, GCPS recommends that the passwords:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Include both numbers and special characters (e.g. @, #, $, *).
- Have a minimum of at least 8 characters and preferably fifteen alphanumeric characters long for a passphrase.
- Should not contain personal information such as a relative or pet's name, social security or driver's license number, street address or phone number, etc.
- Avoid sequences or repeated characters. For example, 1234, 3333, etc.
- Should not be common words such as those found in a dictionary.

GCPS recommends that you select passwords that are unique and not the same as those you use outside of the College. This way if a password on one of your personal accounts has been breached or compromised, the password(s) here at the College remain secure.

A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and

contains a combination of upper and lowercase letters and numeric and punctuation characters. A good passphrase is easy to remember but also secure. The phrase "We're off to see the wizard, The Wonderful Wizard of Oz" can be converted to WotstwTWWoO. Then add some numbers and special characters to make it even more secure.

If a Staff member believes their password has been compromised or made available to others, the Staff member must immediately change their password and notify IT Staff.

7.5 Password Protection Standards

Where possible, do not use the same password for various GCPS access needs. For example, select one password for e-mail systems and a separate password for access to systems that store sensitive or confidential data.

Do not share GCPS passwords with anyone, including Administrative Assistants or Secretaries. All passwords are to be treated as sensitive, confidential GCPS information.

Please remember:

- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not reveal a password to the boss.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.
- Be careful when using social media so that you don't compromise your password.

If someone demands a password, refer them to this document or have them call someone in the IT Department. Do not use the "Remember Password" feature (e.g. browsers, software applications).

Passwords must not be written down. Do not store passwords in a file on ANY computer system or handheld devices without encryption. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all passwords.

7.6 Enforcement

Any Staff member found to have violated this Policy may be subject to disciplinary action, up to and including termination.

8.0 Hardware and software

8.1 Introduction

The presence of a standard Policy regarding the use of software and hardware will:

A. Enhance the uniform performance of the ICT department in delivering, implementing, and maintaining software and hardware suitable to the business needs of GCPS
B. Define the duties and responsibilities of Staff of GCPS who will use the aforementioned software and hardware in the performance of their job duties.

8.2 Definitions

Hardware: The System Unit, Monitor, Keyboard, Mouse and any other additional peripherals such as Printers, Scanners, Modem or Video capture devices.

Software: Any programme or feature requiring set-up or installation of any type. This definition includes, but is not limited to programmes, feature enhancements, upgrades, add-ins, clip-art, etc. This also includes purchased items subject to any licensing agreement, shareware or items distributed for free.

8.3 Purpose of the Hardware and Software Policy

This statement defines and describes GCPS's Policy regarding acceptable usage of the College personal computer hardware and software by the College Staff.
The purpose of this Policy is to:

- ➢ Communicate to Staff the College's requirements regarding the use of computer hardware and software.
- ➢ Facilitate efficient use of GCPS resources

- ➢ Facilitate the Management and support of College owned computer hardware and software.
- ➢ Maintain software standards, ensuring compatibility between College departments.
- ➢ Establish the ownership of the work product created with computer hardware and software as well as responsibilities regarding records retention.

8.4 Acceptable use

This section defines what constitutes "acceptable use" of the College's electronic resources, including software, hardware devices, and network systems. Hardware devices, software programmes, and network systems purchased and provided by the College are to be used only for creating, researching, and processing College-related materials, and other tasks necessary for discharging one's employment duties. By using the College's hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this Policy and other applicable College policies, as well as laws and regulations.

8.5 Violations

Failure to observe these guide Lines may result in disciplinary action by the College depending upon the type and severity of the violation, whether it causes any liability or loss to the College, and/or the presence of any repeated violation(s).

8.6 Software

All software acquired for or on behalf of the GCPS or developed by GCPS Staff or contract personnel on behalf of the College is and at all times shall remain College property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

8.7 Purchasing

All purchasing of College software and hardware shall be centralized within the ICT Department to ensure that all applications conform to corporate software and hardware standards and are purchased at the best possible price. All hardware and software request must be sent through the ICT Department, which will then review the need for such software/hardware, and then determine the standard software/hardware that best accommodates the desired request if ICTdepartment determines that such software is needed.

8.8 Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on College computers. If an employee needs help in interpreting the meaning/application of any such licenses, notices, contracts and agreements, he/she will contact ICT department for assistance. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of the law. In addition to violating such laws, unauthorized duplication of software is a violation of the College Software/Hardware Policy.

8.9 Software Installation

The ICT department is exclusively responsible for installing and supporting all software on College computers. These responsibilities extend to:

- Office desktop computers
- College laptop computers
- PDA devices

9.0 Maintenance

9.1 Introduction

This document describes the fundamental steps to build a consistent ICT maintenance system for GCPS, which are as follows:

- ➢ Maintenance planning and contracting (implement hardware / software / data telecommunications inventories, prioritize needs)
- ➢ Schedule / Monitor Maintenance Activities

Furthermore, the document presents a sample methodology for ad-hoc maintenance Interventions.

9.2. Purpose of the Maintenance Policy

The purpose of this document is to provide best practices and guidelines for scheduling and performing maintenance operations on ICT systems within GCPS.

9.3Target

The primary target consists of System Administrators / I.C.T Team within GCPS, who have the responsibility to schedule and monitor ICT maintenance activities. The secondary target group is all other staff of the College

9.4 Scope

It is in the scope of this document to state the main elements and tasks of ICT maintenance, as well as to provide guidelines for their implementation.

It is out of the scope of this standard to provide:

- ➢ Suggestions for detailed maintenance activities (e.g. how a server or router should be maintained)
- ➢ Template(s) of maintenance contract(s).
- ➢ Describe in detail a Tracking Software Bugs/Problems/Enhancements.

9.5 Type of Maintenance

ICT Maintenance is distinguished as:

- ➢ Preventive, which aims in retaining the system's capabilities before the occurrence of any problem (e.g. system failure).
- ➢ Corrective, which aims in restoring the defective item(s) to the required state.
- ➢ Adaptive, which focus in adjusting a software product to properly interface with a changing environment.
- ➢ Perfective, which refers to enhancements to the product in order to either add new capabilities or modify existing functions.

Preventive and **Corrective** maintenance are both critical factors in maintaining ICT system's availability and performance. Preventive maintenance is usually done in regular time intervals (according to each item's specifications). Ad-hoc preventive maintenance is performed after new software product releases or versions, if they are recommended for bug fixing. Corrective maintenance is required after the occurrence

of a problem or failure, hence the response time of the contractor or the overall availability of the system and its elements are essential indicators and terms in a maintenance contract.

Adaptive maintenance is required mostly in unstable legislative, institutional and/or technical environments. It is performed ad-hoc, in accordance with the frequency the environment changes

Perfective maintenance is normally part of a successful system's life cycle, and refers to further extensions and improvements beyond the initial specifications. It may include the implementation of new software modules and/or new OS and off-the-shelf software versions which aim in performance improvement. In some cases, additional hardware is required to improve system security and performance.

9.6 Process for Maintenance

9.6. 1 Obtain good and detailed system documentation.

A well-documented system (covering the entire architecture as well as all of its elements) is very important, especially for software maintenance. Furthermore, an updated documentation, reflecting the changes derived from the maintenance activities, should be provided for future purposes. Good documentation aims at providing structured instead of unstructured maintenance:

- ➢ Unstructured maintenance wades straight into the source code and makes changes based on that alone
- ➢ Structured maintenance examines and modifies the original design, and then reworks the code to match it

Clearly structured maintenance is a more reliable and (usually) a more efficient process. Unfortunately, it's not possible without detailed design documentation.

9.6.2 Prioritizing needs

Maintenance costs are a significant part of the system's total life cycle costs. Therefore, revision of the business non-functional requirements (such as availability, performance etc) for each part of the system is essential before any signing of a new maintenance contract in order to keep Organization's costs within affordable barriers.

9.6.3 Contracting

Maintenance contracts may be signed with the ICT providers who supplied the equipment/ICT system or third parties who are in possession of the appropriate infrastructure. Increasing the number of contracts and contractors increases

complexity and may cause administrative problems; hence it is advisable to review and consolidate maintenance contracts regularly, possibly achieving significant cost reductions as well.

10.0 Information Security

10.1 Introduction

What is information security and why do we need to think about it?

Information security is the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so. It requires a range of skills and knowledge and increases in importance as our use of and reliance upon information grows. All information has value. Sometimes this might be trivial but in many cases that value is substantial. Value can be measured in different ways, depending on the nature of information. In some cases, there may be a straight forward monetary value associated with given information. For others, emphasis is placed on different aspects of value.
For example, the effects of unauthorized disclosure and loss of confidentiality. The range of undesirable consequences associated with breaches of information security is long and includes:

- systems being unavailable;
- bad publicity and embarrassment;
- fraud;
- illegal personal investigation;
- industrial espionage.

How can information be protected?

Information security can be a daunting prospect for the average user. It is often seen as a highly technical discipline that requires expensive equipment and specialist assistance. While there are many situations that do need this type of approach, the most sensible and effective first steps are based on common sense and sound Management practice. Assessing and understanding the risks for our own organisation will help to establish appropriate risk Management. In turn, this should ensure appropriate incident Management and recovery when security is compromised.

For organisations of higher and further education a good level of information security can be achieved through the
following:

- ➢ A pragmatic approach to Policy and standards should be adopted resulting in an information security Policy, which is supported by realistic and workable processes and procedures.
- ➢ The rigour of security measures applicable to any information system should be proportional to the assessed risk of the confidentiality, integrity or availability of its information becoming compromised.
- ➢ The risk assessment process should be light touch and might categorise the likelihood and consequences of any compromise of an information system's confidentiality, integrity or availability as being high, medium or low.
- ➢ A well informed, well trained workforce, who exercise an appropriate (but not excessive) level of vigilance, is an essential element of any security package

10.2 Purpose of Information Security Policy

This Policy provides a framework for the Management of Information Security throughout the College. It applies to:

1. all those with access to College information systems, including staff, residents , and visitors
2. any systems attached to the College computer or telephone networks and any systems supplied by the College
3. all information (data) processed by the College pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the College and any College information (data) held on systems external to the College's network
4. all external parties that provide services to the College in respect of information processing facilities and business activities and
5. principal information assets including the physical locations from which the College operates.

10. 3 Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information.

The framework for managing information security in this Policy applies to all GCPS entities and workers, and other Involved Persons

10.4 Aims and Commitments of Information Security

The College recognizes the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and

information systems underpin all the College's activities, and are essential to its research, teaching and administrative functions.

Any reduction in the confidentiality, integrity or availability of information could prevent the College from functioning effectively and efficiently. In addition, the loss or unauthorized disclosure of information has the potential to damage the College's reputation and cause financial loss

To mitigate these risks, information security must be an integral part of information Management, whether the information is held in electronic or hard-copy form.

The College is committed to protecting the security of its information and information systems in order to ensure that:

1. the integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose';
2. information is always available to those who need it and there is no disruption to the business of the College;
3. confidentiality is not breached, so that information is accessed only by those authorised to do so;
4. the reputation of the College is safeguarded.

In order to meet these aims, the College is committed to implementing security controls that conform to best practice, as set out in the *ISO/IEC 27002:2005 Information Security Techniques – Code of practice for information security Management*

Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

The College is committed to providing sufficient education and training to users to ensure they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information.

Specialist advice on information security shall be made available throughout the College.

An Information Security Advisory Group (or groups), comprising representatives from all relevant parts of the College, shall advise on best practice and coordinate the implementation of information security controls.

The College will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security Policy.

Breaches of information security must be recorded and reported to appropriate bodies in the College, who will take action and inform the relevant authorities

This Policy and all other supporting Policy documents shall be communicated as necessary throughout the College to meet its objectives and requirements.

10.5 Risk Assessment and Management

10.5.1 Risk assessment of information held

The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

The risk assessment should identify the department's information assets; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to the department or College as a whole. In assessing risk, departments should consider the value of the asset, the threats to that asset and its vulnerability.

Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

Rules for the acceptable use of information assets should be identified, documented and implemented.

Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the College's infrastructure, systems and processes.

10.5.2 Risk Management

A thorough analysis of all GCPS information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information.

The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource.

The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats.

Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

10.6 Protection of confidential information

Identifying confidential information is a matter for assessment in each individual case. Broadly, however, information will be confidential if it is limited to public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorized disclosure could have one or more of the following consequences:

1. financial loss
   e.g. the withdrawal of a research grant or donation, a fine by the ICO, a legal claim for breach of confidence;
2. reputational damage
   e.g. adverse publicity, demonstrations, complaints about breaches of privacy; and/or
3. an adverse effect on the safety or well-being of members of the College or those associated with it
   e.g. increased threats to staff or residents engaged in sensitive research, embarrassment or damage to benefactors, suppliers, staff and residents

10.6.1 Storage

Confidential information should be kept secure, using, where practicable, dedicated storage (e.g. file servers) rather than local hard disks, and an appropriate level of physical security.

File or disk encryption should be considered as an additional layer of defense, where physical security is considered insufficient.

10.6.2 Access

Confidential information must be stored in such a way as to ensure that only authorized persons can access it.

All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords.

Where necessary, additional forms of authentication should be considered.

To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.

Users with access to confidential information should be security vetted, as appropriate, in accordance with existing policies.

Physical access should be monitored, and access records maintained.

10.6.3 Remote Access

Where remote access is required, this must be controlled via a well-defined access control Policy and tight access controls provided to allow the minimum access necessary.

Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

10.6.4 Copying

The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where necessary, a record kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed .

All copies should be physically secured e.g. stored in a locked cupboard drawer or filing cabinet.

10.6.5 Cryptographic Controls

Procedures should be in place to support the use of cryptographic techniques and to ensure that only authorised personnel may gain access to confidential information.

10.8.6 System Planning and Acceptance

A risk assessment should be carried out as part of the business case for any new ICT system that may be used to store confidential information. The risk assessment should be repeated periodically on any existing systems.

10.7 Backup

Information owners should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken and tested regularly in accordance with such an appropriate backup Policy.

10.9 Compliance

The College has established this Policy to promote information security and compliance with relevant legislation. The College regards any breach of information security requirements as a serious matter, which may result in disciplinary action.

Compliance with this Policy should form part of any contract with a third party that may involve access to network or computer systems or data.

11.0. MISCELLANEOUS

11.1 Portable Equipment and Remote Working

Portable equipment owned by the College may include laptop computers, blackberries, mobile telephones with email capability, etc. Computer equipment should not be removed from the College without the prior approval of your Head of ICT Department. It is particularly emphasised that you must follow agreed back-up procedures to protect any information that you create on any portable device. When working away from your normal place of work (e.g. travelling, working from home or from a different venue), there are increased ICT security measures that should be adhered to:

- ➢ check the location and direction of your display to ensure confidential information is out of view of others
- ➢ ensure that data printed is collected and stored securely
- ➢ ensure that any systems containing College data are password protected (in the case of computers) or PIN protected (in the case of mobile telephones)

If you are issued with a cellular network 'dongle' to enable you to access the Internet while away from your normal workplace, please note that the cost of Internet access can be very high; this is therefore to be used for essential business purposes only, especially if abroad. If an item of portable equipment is lost or damaged due to an act of negligence, the individual responsible will be expected to fully explain the loss or damage to the satisfaction of the College and may be asked to meet a proportion of the loss or damage, up to and including the full sum involved. These cases will be considered on an individual basis, and it is expected to involve the supervising Head of ICT Department

11.2 Installing Software:

Get permission from ICT Dep't before you install any software (including public domain software) on equipment owned and/or operated by GCPS.

11.3 Use of office Devices for leisure:

Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, playing computer games and browsing the Internet) is permitted so long as such use does not:

- incur specific expenditure for GCPS
- impact on your performance of your job (this is a matter between each member of staff and their Line Manager)
- bring GCPS into disrepute.

Playing Computer games and watching movies is strictly not allowed. Such activities can attract sanctions.

11.4 Care of office equipment:

- Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting ICT Department
- Don't take food or drink into rooms which contain specialist equipment like servers .Access to such rooms are limited to systems administrators and other authorised staff.

11.5 Data Centre / Server Room Access

Only authorised ICT personnel are allowed to access the ICT data center / Server room. All other persons must be accompanied by authorised staff.

11.6 Printers, Telephone Lines, Fax and Copiers.

Staffs are expected to use Printers, Telephone lines, Fax and Copiers responsibly**.** Irresponsible/ excessive use of the above for personal purposes is discouraged, and may, depending on the Line Manager's determination and Management's approval lead to disciplinary action which may include, but not limited to, denial of the service.

11.7 ICT Technical Assistance Request & Complaints.

All ICT technical assistance requests shall be made to the ICT Department by filling a computer repair request form before any assistance could be carried out .

Staff requesting for the technical support shall complete the same form and sign after the assistance is rendered.

This form shall be kept by the I.C.T Manager for record keeping purposes

11.8 Antivirus

The College through the assistance of the ICT Department will have to buy a licensed antivirus for all Computers on the College network in order to protect all systems and secure the internal network. This license should be renewed yearly or as soon as they expire.

11.9 Back up and Data Recovery

The ICT Department will have to put measures in place to back up all College data on a centralised server within the College as well as outside the College to protect the data against moments of fire or any natural disasters. All staff members will be educated on how to play their part in helping the backing up process of various departmental data.

In times of Disaster, the College will fall on the "I.C.T DISASTER RECOVERY AND SERVICE CONTINUITY PLAN " that will be develop by the I.C.T team to outline the role and the procedure the I.C.T/individual staff will play to restore I.C.T service within the College.

11.10 Access of College Computers by Non staff

It is strictly prohibited for any non-staff member of the College to use office computers for whatever business activity. Officers who allow their office computers to be used in such a situation will be charged and punished with the appropriate punishment sanctioned by management

This is to protect the confidentiality of the College data and systems. However the College shall make available Guest Computer(s) at the Library that could be used by non-staff members who visit the College.

12.0. Revision of the Policy

This Policy shall be revised every two(2) years . Changes necessitating revision shall include changes in technology, statutory regulations and any other reasons as may be determined from time to time by the Manager in charge of ICT.

BIBLIOGRAPHY

1. Kenya Electricity Generation Company Limited , KENGEN I.C.T POLICY 2008
2. Wirral Metropolitan College Student I.C.T usage Policy 2007
3. Exeter College I.C.T and Computer usage Policy document , 2010

Prepared By:

I.C.T MANAGER
GCPS

Signature & Date:

_____

Authorized By:

_____