INTEGRI PROCEDAMUS

UNIVERSITY OF GHANA SPECIAL REPORTER

PUBLISHED BY AUTHORITY

NO. 968 JUNE 24, 2022 VOL. 59 NO. 9

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

UNIVERSITY OF GHANA

INTEGRI PROCEDAMUS

Information and Communication Technology Policy

May 2022

TABLE OF CONTENTS

PREAMBLE

The University of Ghana (UG), a premier state funded research-intensive university, consists of four (4) colleges, ten (11) learning centres and several research institutions and centres.

Within the nine (9) key priorities of University of Ghana's strategy for attaining world-class status, lie the institutional processes which emphasize overhauling all governance arrangements to achieve greater effectiveness and efficiency. Underpinning this priority is the objective of modernizing management systems and processes using an integrated ICT approach. In this context, ICT is identified to be the foundation in maximizing student, faculty, and staff productivity, ensuring efficient service delivery, enhancing teaching, and learning and improving quality of research. Against this background, the University of Ghana Computing Systems (UGCS) has taken up the mandate of developing policy documents that will guide the development, implementation, and effective use of the ICT resources within the University. These set of policies will function side by side with other related published documents as the reference document on standard procedures and guidelines used within the University of Ghana.

PURPOSE

Among relevant legal legislation and documentation governing the state of Ghana such as the Electronic Transaction Act, 2008 (Act 772), the Electronic Communication Act, 2008 (Act 775), the Data Protection Act 2012 (Act 843), organizations and universities alike are urged to solicit, hold, use, and protect all information resources in their custody appropriately. The Cybersecurity Act 2020, (Act 1038) designates public universities as national critical information infrastructure. It is therefore very essential to enact these policies for the following reasons:

i. To ensure smooth operations of ICT infrastructure and access to internet.
ii. To protect UG's sensitive information from unauthorized access.
iii. To ensure all users have adequate and available electronic resources for their work.

iv. To be cost efficient by standardizing the ICT procurement and maintenance process.
v. To enforce and ensure minimum information & network security standards to prevent any misuse from UG's own users and outsiders .
vi. To protect UG's ICT assets from cyber related attacks and to prevent it from being used as a platform to create a cyber-attack somewhere outside the campus.
vii. To promote collaborations between industry and academia through effective electronic communications.

SCOPE

This Policy applies to all users accessing ICT resources and any third party who has been authorized to use ICT resources within the University. This policy framework shall be used in conjunction with supporting guidelines, procedures and codes of practice developed as it becomes necessary and published on the UGCS website.

Scope of the Policy in respect of electronic transactions

(1) This Policy applies to electronic transactions and electronic records of every type.
(2) This Policy shall not be interpreted to exclude statute law, or the principles of the common law being applied to, recognizing, or accommodating electronic transactions, electronic records or any other matter provided for in this Policy.
(3) Unless otherwise provided, this Policy shall not be construed as requiring a person to generate, communicate, produce, process, send, receive, record, retain, store or display information, document, or signature by or in electronic form
(4) This Policy does not limit the operation of law that expressly authorizes, prohibits, or regulates the use of electronic records and any legal requirement for information to be posted, displayed, or transmitted in a specified manner

REVIEW

Due to the fast pace of technology, this Policy shall be reviewed and updated every three (3) years. However, any legislative, and unforeseeable changes affecting this Policy may trigger a review process to commence.

REVISION HISTORY

Version	Date	Change Description	Author
0.1	February 2014	First Draft	Mawuli Takpo
0.2	June 2014	Draft Review	Head, Information Technology (IT) Planning & Security
0.3	December 2015	Content Review	Deputy CITO IT Planning, Security and Support
0.4	March 2016	Content Review	Prof. H. A Yitah
0.5	December 2016	Content Review	Deputy CITO IT Planning, security and Support
0.6	April 2017	Vice Chancellor's Committee Review	VC's Committee
0.7	May 2017	Contents Review Update	Head IT Planning & Security
0.8	May 2017	Content Review	Director, Public Affairs Directorate
0.9	June 2017	Content Review	Prof. Christopher Gordon
1.0	June 2017	Content Review Update	CITO
1.1	April 2021	Review	Business and Executive Com-mittee
1.2	October 2021	Periodic Review	CITO
1.3	November 2021	Content Review	IT Management Board
1.4	November 2021	Content Review	Chief Risk Officer
1.5	February 2021	Content Review	Legal Counsel
1.6	February 2022	Final Content Review	CITO

GLOSSARY/DEFINITION OF TERMS

Term	Definition
Act	The Data Protection Act, 2012 (Act 843); Cybersecurity Act, 2020 (Act 1038); Electronic Transactions Act, 2008 (Act 772).
Authentication	The process of verifying the authenticity of the person requesting access to a network before being granted access.
Authority	Means the Cyber Security Authority set up under Act 1038.
Availability	Ensuring that authorized users always have access to ICT resources when they need it
Backup Media	Storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, hard drives, or cloud storage.
Backup	Refers to snapshots taken of the file structure and database for the sole purpose of keeping data of that snapshot safe.
BYOD	Personally owned electronic devices that users are permitted to bring to work or use to access University of Ghana information resources regardless of the location of the user.
Chain Letters	Letters that promise some form of reward when forwarded to several users.
Computer Security Incident	Any event that threatens the confidentiality, integrity, or availability of university systems, applications, data, or networks. University systems include, but are not limited to servers, desktops, laptops, workstations, tablets, smart devices, network servers/ processors, or any other electronic data storage or transmission device.
Commission	Means the Data Protection Commission established under the Data Protection Act, 2012 (Act 843)

Confidential Data Security Incident	A subset of Computer Security Incidents that specifically threatens the security or privacy of Confidential University Data.
Confidential Data	Any data, the unauthorized disclosure, alteration, or destruction of which could cause a significant level of risk to the University or its affiliates. Examples of confidential data include data protected by the country's privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to confidential data.
Confidentiality	Ensuring that information is accessible to only authorized personnel.
Credentials	Any evidence of access such as passwords, personal identification number, token, biometric, etc.
Critical Services	Any service whose 'failure' or compromise could threaten human life, the system's environment or the reputation and existence of the University
Critical systems	Any system whose 'failure' or compromise could threaten human life, the system's environment or the reputation and existence of the University
Data Controller	Any person who determines the purposes for which any personal data are to be processed
Data Custodian	An entity who is responsible for the safe custody, transport, and storage of the data.
Data Owner	An entity with the overall responsibility for the accuracy, integrity, and availability of data.
Data Processor	Any person other than an employee of the data controller who processes the data on behalf of the data controller.

Data Protection Supervisor	A professional appointed by the data controller to monitor compliance by the data controller in accordance with the provisions of the Data Protection Act.
Data Subject	The data subject is the individual whom the personal data is about.
Electronic Devices	Laptops, desktops, tablets, smart phones.
Encryption	It is the method of encoding information in a manner that makes it unintelligible to anyone else.
Full Backup	A backup that makes a complete copy of the data since the last backup.
ICT	Information and Communication Technology
ICT Resources	Computing equipment, communication equipment and software applications provided to support the learning, teaching, research, and administration functions of the University of Ghana.
Integrity	Safeguarding data accuracy and its completeness.
Internal Only Data	Any data, the unauthorized disclosure, alteration, or destruction of which could result in a moderate level of risk to the University or its affiliates. All institutional data that is not explicitly classified as confidential or public data should be treated as internal only data. A reasonable level of security controls should be applied to internal only data.
MAC	Media Access Controller
Misuse	Any action intended to wilfully compromise a system or steal information with or without appropriate authorization
Network Scanning	A procedure for discovering active hosts on a network, either for attacking them or for assessing their security vulnerabilities

Off-site	A secure location for storing backup media, which is geographically separate from the primary location housing the information system that is being backed up.
Personal Data	Data about an individual who can be identified, from the data, or from the data or other information in the possession of, or likely to come into the possession of the data controller.
Processing	Any way in which data is handled including collecting, viewing, analysing, storing or destroying.
Policy Records	Academic board minutes, University Council minutes, Business and Executive Committee minutes, College minutes, and any constituted committee minutes within the University.
Ponzi Schemes	Fraudulent investment operations.
Proprietary Infor-mation	Data, information, or intellectual property in which the University has an exclu-sive legal interest or ownership right, which, if compromised, could cause significant harm to UG. Examples may include, but are not limited to, business planning, financial information, trade secret, copyrighted material, and software or comparable material from a third party when the University has agreed to keep such information confidential.
Public Data	Any data the unauthorized disclosure, alteration, or destruction of which would results in little or no risk to the University and its affiliates. Examples of public data include press releases, course information and research publications.
Pyramid Scheme	A Ponzi scheme model that promises payments based on an individual enrolling other people.

Replication	Refers to the copying process of all data from the primary location to a secondary location for keeping a mirrored copy of the live data.
Resource Owner	Any person capable of granting access to a protected resource.
Restoration (Recovery)	The process of restoring the data from its backup state to its normal state so that it can be used and accessed in a regular manner.
Reviewing Panel	Means a panel comprising the creator of a record, a representative of the Legal Counsel and UGCS, the University Archivist constituted to review retained records pursuant to the provisions of this Policy.
Sensitive Personal Information	Information relating to an individual that identifies the individual and, if compromised, could cause significant harm to that individual or to UG. Examples may include, but are not limited to: Social Security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information UG has promised to keep confidential, and account passwords or encryption keys used to protect access to Confidential University Data.
Service Set Identifier (SSID)	A unique identifier that user wireless devices use to associate with Wireless Access Points
Spam	Unsolicited bulk email.

Special Personal Data	Personal data which consists of information that relates to:` (a) the race, colour, ethnic or tribal origin of the data subject. (b) the political opinion of the data subject. (c) the religious beliefs or other beliefs of a similar nature, of the data subject. (d) the physical, medical, mental health or mental condition or DNA of the data subject. (e) the sexual orientation of the data subject. (f) the commission or alleged commission of an offence by the individual; or (g) proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in the proceedings
System Abuse	When a person indulges in unacceptable use or practices that would make the University's ICT infrastructure vulnerable to cyber-attacks.
System Administrator	Technical persons with the overall responsibility for handling computer systems and backing up information systems.
System Controller	The person (or persons) with the responsibility for the day-to-day operation, con-trol, and maintenance of an information system.
System Operator	An entity who manages the operation of an ICT system or service.
System Owner	The person (or persons) with overall responsibility for a system and its data as a university asset.
System	A computer that provides a service, other than simple desktop use, to more than a single person
Third Party	Anyone who is not the system administrator responsible for the day-to-day back-up of the data.

User	Staff, students, faculty, and any other person authorized to use University of Gha-na ICT resources including ICT personnel, third party contractors etc.
VoIP (Voice Over Internet Protocol)	Voice over Internet Protocol

ACCEPTABLE USE POLICY

Overview

The University of Ghana (UG) is committed to protecting members of its community, including employees, students, and affiliated members, from damaging or illegal actions related to ICT resources. Users are encouraged to use the ICT resources in line with the mission of the University to further the goals and objectives of their work, study, or research.

Purpose

The Acceptable Use Policy seeks to outline the acceptable use of information and communication technology and related resources within the University of Ghana (UG) and to inform the University users of the regulations relating to the use of information and communications technology resources. Inappropriate use of these resources can expose University of Ghana to legal liabilities and system compromise including reputational damage and security breaches.

Policy

All users of the University's ICT resources shall be duly registered on the University's identity management system, authenticated, and appropriately authorized to use such resources. Usage of ICT resources shall be done in a manner to promote the mission of the University.

General Use and Ownership

i. All users shall comply with existing University policies. It is important that all members of the University acquaint themselves with the existing policies.

ii. Users shall not access, interfere with, or remove any ICT facility, data, or information unless they have been authorized to do so.

iii. Users shall be given access to use ICT facilities in a manner that is consistent with their role.

iv. All use of ICT facilities shall be lawful, honest, and decent and with due regard for the rights and sensibilities of other people.

v. Users are responsible for appropriate use of all resources assigned to them. Authorized users of University of Ghana ICT resources shall not allow unauthorized users to access the network in any way.

Security Information

i. Users shall not use ICT resources in a way that deliberately disrupts the use of such resources.

ii. Users are responsible for ensuring that their devices are always protected from cyber-attacks

iii. All ICT resources connected to University ICT infrastructure shall be identified and authenticated.

iv. Users shall not deliberately create, use, or distribute materials that could bring the University into disrepute.

v. As part of the UGCS mandate, authorized University administrators shall monitor electronic data held on or transmitted through the University ICT infrastructure.

vi. Users shall protect their credentials against misuse and secure resources against unauthorized use or access.

vii. Multifactor authentication is a primary means of authentication on university systems to mitigate against impersonation and cyber related activities.

viii. Personnel shall be trained appropriately in processing data especially those whose role bothers on processing confidential or sensitive data. Data shall be appropriately labelled according to the HRODD policy to prevent breaches.

ix. Privacy notices shall be developed and published to inform the public on how the University processes personal data of its data subjects. Surveillance installations shall be accompanied by privacy notices.

x. Users shall take the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical, and organizational measures to prevent:
   a. loss of, damage to, or unauthorized destruction; and
   b. unlawful access to or unauthorized processing of personal data.

xi. To comply with the above, the University shall take reasonable measures to:
   a. identify reasonably foreseeable internal and external risks to personal data under that person's possession or control;
   b. establish and maintain appropriate safeguards against the identified risks;
   c. regularly verify that the safeguards are effectively implemented and;
   d. ensure that the safeguards are continually updated in response to new risks or deficiencies.

xii. Users shall observe all generally accepted information security practices and procedure and specific industry or professional rules and regulations

xiii. Users who process personal data on behalf of the University or authorizes others to do so shall:
   a. process the data only with the prior knowledge or authorization of the University, and
   b. treat the personal data which comes to their knowledge as confidential.

xiv. A person who processes personal data on behalf the University shall not disclose the data unless
   a. required by law, or
   b. in the course of the discharge of a duty.

xv. The University shall not disclose personal data which relates to the physical, mental health or mental condition of the data subject, unless the disclosure is required by law

xvi. A User shall not sell or offer to sell personal data of another person. A User who contravenes this provision commits an offence and shall be liable to the extent provided by the Act.

Notification of Security Compromise

Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorized person, the User who processes data under the authority of the University shall notify the University through the University's Data Protection Supervisor for onward notification of the Commission and the data subject of the unauthorized access or acquisition.

i. The notification shall be made as soon as reasonably practicable after the discovery of the unauthorized access or acquisition of the data.

ii. The University shall take steps to ensure the restoration of the integrity of the information system.

iii. The University shall delay notification to the data subject where the security agencies or the Commission inform the University that notification may impede a criminal investigation.

iv. The notification to a data subject shall be communicated to the data subject by

   (a) registered mail to the last known residential or postal address of the data subject;

   (b) electronic mail to the last known electronic mail address of the data subject;

   (c) placement in a prominent position on the website of the responsible party;

   (d) publication in the media; or

   (e) any other manner that the Commission may direct.

   v. A notification shall provide sufficient information to allow the data subject to take protective measures against the consequences of unauthorized access or acquisition of the data.

vi. The information shall include, if known to the data controller, the identity of the unauthorized person who may have accessed or acquired the personal data.

Duty of the University as an owner of critical information infrastructure to report a cybersecurity incident.

i. The University as a critical information infrastructure shall:

   a. Report a cybersecurity incident within twenty-four hours after the incident is detected to

      1. the relevant Sectoral Computer Emergency Response Team as established by the Cybersecurity Act, 2020 (Act 1038); or
      2. the National Computer Emergency Response Team, in the case of a critical information infrastructure that does not belong to a Sectoral Computer Emergency Response Team as established by the Cybersecurity Act, 2020 (Act 1038);

   b. Cause an audit to be performed on a critical information infrastructure and

   c. Submit a copy of the audit report to the Cyber Security Authority (the Authority).

ii. Any person or officer of the University who contravenes the provisions in the preceding paragraph 1 and subparagraphs, shall be liable to pay to the Authority the administrative penalty specified in the Second Schedule of Act 1038 imposed on the University by the Authority as a result of the contravention.

Access to Communication

i. UG Email is the official method of communication for both students and employees.

ii. A VoIP system is used to facilitate direct communication (audio or video calls) within the UG community and outside the institution.

iii. Video Conferencing equipment is used primarily for instructional classrooms requiring connectivity to other UG locations such as research and regional centres. It is also used to facilitate conferences and meetings with other third party entities.

iv. Microsoft Teams harnesses VoIP, video conferencing and collaboration into one application. It is used to facilitate communication within the University and with other third parties.

v. Social Media is one of the tools used to communicate the University position on a myriad of issues and shall be used in line with University guidelines on social media. Personal statements concerning University matters on media platforms shall be prefixed with the appropriate disclaimer.

vi. Sakai is the official online learning management software tool for teaching and learning. Other online collaboration tools such as Microsoft Teams, Google Meet and Zoom may be used to support the learning management software.

vii. In the case of those with visual related impairments, the Fusion software is the prescribed technological intervention.

viii. Messaging tools such as WhatsApp allow for fast dissemination of information. They however lend themselves to leakage of proprietary or confidential information and have no institutional history because the data is stored on devices of private individuals. Decisions taken during discussions, meetings and collaborative efforts on these platforms shall always be communicated using email or be physically documented.

Unacceptable Use

The list below is by no means exhaustive, but attempts to provide a framework for activities, which fall into the category of unacceptable use.

i. Under no circumstances is a user of the University's ICT resources authorized to engage in any activity that is illegal under local and international law including cybercrime, crypto mining, and cyber bullying.

ii. Users shall not give their account credential such as passwords or personal identification numbers (PIN) to others or allow the use of their accounts by others including family and other household members.

iii. Users shall not breach security or disrupt network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless such activities are within the scope of regular duties.

iv. Executing any form of UG infrastructure reconnaissance and monitoring is prohibited unless this activity is a part of the user's normal duty or unless prior notification is given to University of Ghana Computing Systems.

v. Users shall not circumvent the authentication or security mechanisms of any device, network or account controlled by the University.

vi. Sending unsolicited email messages or other advertising material to users who did not specifically request such material is prohibited.

vii. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited

viii. Users shall refrain from connecting network devices unto the UG network without authorization.

ix. Usurping the University's bandwidth for commercial purposes or personal interest is prohibited.

x. A user shall not access another user's account without authorization.

xi. A user shall not transmit University confidential data to any external source.

xii. Using personal mails for university business is prohibited.

Processing of Special Personal Data

The University shall not process personal data which relates to:

i. (a) a child who is under parental control, or

(b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behaviour of an individual.

ii. The University as a data controller may process special personal data in accordance with the Act where
(a) processing is necessary, or
(b) the data subject consents to the processing.

iii. The processing of special personal data is necessary where it is for the exercise or performance of a right or an obligation conferred or imposed by law on the University in its capacity as an employer.

iv. Special personal data shall not be processed unless the processing is necessary for the protection of the vital interests of the data subject where
(a) it is impossible for consent to be given by or on behalf of the data subject,
(b) the University cannot reasonably be expected to obtain the consent of the data subject, or
(c) consent by or on behalf of the data subject has been unreasonably withheld.

v. Special p ersonal data shall not be processed unless the processing is carried out for the protection of the legitimate activities of a body or association which
(a) is established for non-profit purposes,
(b) exists for political, philosophical, religious or trade union purposes;
(c) relates to individuals who are members of the body or association or have regular contact with the body or association in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

vi. The processing of special personal data shall be presumed to be necessary where it is required
(a) for the purpose of or in connection with a legal proceeding,
(b) to obtain legal advice,
(c) for the establishment, exercise or defence of

legal rights,
(d) in the course of the administration of justice, or
(e) for medical purposes and the processing is undertaken by a health professional, and pursuant to a duty of confidentiality between patient and health professional. “Medical purposes” includes the purposes of preventive medicine, medical diagnosis, medical research, provision of care and treatment and the management of healthcare services by a medical or dental practitioner or a legally recognized traditional healer.

vii. The University shall not process special personal data in respect of race or ethnic origin unless the processing of the special personal data is necessary for the identification and elimination of discriminatory practices, and carried out with appropriate safeguards for the rights and freedoms of the data subject

Communication Privacy

The University shall not, without user permission, monitor, review or otherwise access communications sent or received (e.g., email), created or stored on Information Technology Resources, except for reasons below which permits access when determined reasonable by a senior administrative officer. These reasons include but are not limited to the following:

i. To comply with a subpoena, warrant, court order, law enforcement or similar legal process.

ii. During investigation or prevention of a violation of the University’s policy or law

iii. Protect health and safety and assurance that harm has not occurred to a user.

iv. To minimize computer activity that interferes with the University’s infrastructure or service.

v. UGCS may use tools to manage its operations, including (but not limited to)

   a. spam,

   b. malware detection,

c. elimination, limitation of network volume or blockage of access to specific file types or sites, or

d. restriction of access to sites that present a security risk to the University's systems.

Complete privacy is not assured when using the University ICT resources.

Consequences of Misuse of Computing or Network Privileges

Users who breach this policy may be subject to disciplinary and legal action by authorities of University of Ghana.

Cooperation Expected

Users, when requested, are expected to cooperate with UGCS in any investigation of system abuse.

Users who have been victims of abuse may contact the University of Ghana Computing Systems through one of the following service desk channels:

i. Use call IP phone: 3000 between 9 a.m. and 5 p.m. Monday-Friday.

ii. Email: servicedesk@ug.edu.gh

iii. Visit the UGCS Service Desk located on the ground floor in the UGCS Building.

Ownership

The University Council owns this policy. The Chief Information Technology Officer (CITO) of University of Ghana Computing Systems is responsible for maintaining this policy and providing guidance and advice on its implementation.

EMAIL POLICY

Purpose

The purpose of this policy is to facilitate effective electronic mail or email communications and to reduce risks relating to email usage. The policy prescribes the rules for using, managing, and constructing emails for the protection of the University and all other interested parties.

Scope

This policy applies to all users of the University of Ghana. The policy concerns all electronic mail sent or accessed from the University of Ghana network.

Policy

The University community shall use the approved official email of the University to conduct University related business always. Using personal mails for university business is prohibited.

Proper Use of University of Ghana Email Systems

For this policy, UG community members are classified into the following five (5) categories.

i. Junior Members (Students)
ii. Junior Staff
iii. Senior Staff
iv. Senior Members
v. Guests (national service personnel, attachment personnel, temporary staff, visiting scholars, external partners)

The official suffix for University of Ghana email is “ug.edu.gh” for all categories except students and guests. For students, the suffix is “st.ug.edu.gh.” For guests, the suffix is “staff.ug.edu.gh”

Upon joining the University, a user shall be given a University of Ghana email account and address. This email account shall be used by the University for a variety of essential and official communications with members of its community.

Users shall be responsible for operating and managing their email accounts and shall exercise good judgement when sending or receiving email on the University’s network. The following are guidelines for the proper use of the University email system.

Sending Email

i. Composition

An email is an official document which shall be carefully composed, addressed, and sent to only the appropriate recipient(s).

ii Attachments

Email attachments are limited to 10Mbytes. Where an attachment exceeds this limit, users shall use the established UG shared folder or Microsoft OneDrive or SharePoint

iii Group Mails/Distribution Lists

a. Users may send official emails to distribution groups to which they belong.

b. Emails targeted at a specific audience (example University Teachers Association of Ghana (UTAG), etc.) shall be directed to that specific distribution list.

c. Users who belong to a specific group (example UTAG, etc.) shall subscribe directly or contact their group leader to ensure they are added to the group distribution list.

d. Group mails targeting all staff of the University community shall be authorized by the Public Affairs Directorate while those intended for all students shall be authorized by the office of Dean of Students Affairs.

e. Email communications from an outside group or unit, requires the explicit approval of the administrator of that group or unit. It is the responsibility of the sender/requestor of a group email to obtain the necessary approval from the administrator of that group or their designee.

f. Group owners, leaders or administrators shall be responsible for managing their group lists including ensuring that membership is current. Any list that becomes redundant (duration of a semester) shall be removed by the domain administrator without notice.

g. Group owners shall be automatically deemed as moderators of a group. They shall be accountable for posts within their groups and are urged to empower their groups on the content of posts to prevent posting of fake news and unwholesome content. Groups that target like-minded professionals such as UTAG, TEWU (Teachers and Educational Workers Union), etc. may opt to have a peer-policing moderation policy however, for groups such as UGSTAFF that target a diverse section of the community, moderation is mandatory.

iv. Personal marketing and advertising emails

a. Personal marketing and advertising emails shall be sent to the University marketplace on Microsoft (MS) SharePoint.

b. Institutional marketing and advertising emails targeted at the entire University shall be sent by the Public Affairs Directorate

v. Email Retention Period

a. Staff who retire from the University of Ghana shall keep their email address until Human Resource and Organizational Development Directorate (HRODD) notifies UGCS otherwise.

b. University staff who abandon their posts or resign, or whose contracts have been terminated, shall have their accounts disabled immediately and deleted after ninety (90) days per HRODD notification.

Personal Use and General Guidelines

Personal use of the University email system is permitted so long as such usage does not interfere with the user's job responsibilities or expose the University to security risks.

Business Communications and Email

Email is an official method of communication to members of the UG community. In this regard, every member of staff and admitted student shall be provided with a UG email address for communication.

Email Signature

UG email users shall comply with the following email signature below:

i. User's full name and Title (Optional)

ii. Job title

iii. Institution (college, school, directorate, department, institute, centre)

iv. Institution Address

v. Telephone number (Office Phone, IP Phone, Cell Phone (Optional))
vi. UG website address.
vii. UG Social Media Sites (LinkedIn, Twitter)

Email Forwarding

As part of efforts to secure the community email from social engineering attacks such as phishing, the community is restricted from forwarding their UG emails to their personal external email services. This is to mitigate cybersecurity risks of phishing which leads to account compromise and intrusions.

External Email Accounts

Using personal external email accounts to conduct University of Ghana business is prohibited.

Students Email Accounts

All students shall be provided official email accounts as part of their enrolment into the University. It is the responsibility of the student to activate their email addresses. All official electronic correspondence from the University shall be channelled only through UG email accounts. Students are responsible for ensuring their official email addresses are active always.

Students Alumni Accounts

Students who have graduated from the University may continue to use their email address. All alumni email addresses shall, however, be moved into an alumni distribution list to ensure they do not receive active student email correspondence.

Email Disclaimers

The following disclaimer shall automatically be included as a suffix to all email messages to addresses external to the University of Ghana. Users shall consider the implication of the disclaimer.

Email Disclaimer:

---------- DISCLAIMER -------

This email, its attachments and any rights attaching hereto are, unless the context clearly indicates otherwise, the property of University of Ghana. It is confidential and intended for the addressee only. If you are not the addressee and have received this email by mistake, kindly notify the sender and delete this email immediately. Do not disclose or use the email in any manner whatsoever. Views and opinions expressed in this email are those of the sender unless clearly stated as those of the University of Ghana. The University of Ghana accepts no liability whatsoever for any loss or damages, however incurred, resulting from the use of this email or its attachments. The University of Ghana does not warrant the integrity of this email, nor that it is free of errors, viruses, interception, or interference.

Enforcement

This policy shall be enforced by UGCS. Users who breach this policy may be subject to disciplinary and legal action by authorities of University of Ghana.

BRING YOUR OWN DEVICE (BYOD) POLICY

Purpose

University of Ghana recognizes the benefits that may be derived from allowing users to bring their personally owned electronic devices to work, and to use such devices to process University information regardless of location. Such devices are handy but may also introduce malware and other undesirable security risks into the University network. Additionally, such devices are susceptible to loss or theft. The purpose of this policy is to protect University of Ghana ICT resources. This policy specifies how personally owned electronic devices may be used.

Scope

This policy applies to all personally owned electronic devices that are used to access, transmit, receive, and store University information. The policy is applicable to all users of the University community.

Policy

The University of Ghana shall accommodate users who intend and or use their own devices for work purposes; however, the University shall take all necessary measures to protect its resources on that device. The University shall provide all resources necessary to protect its data and infrastructure. All university related data shall be stored in the University's approved storage (MS OneDrive) which comes with the official Microsoft productivity suite.

Devices and Support

i. All users shall be properly authenticated through the University's official authentication system to access the University's network

ii. All smart or network-enabled devices shall be registered and authenticated prior to using the University's infrastructure.

iii. Network connectivity issues are supported by University of Ghana Computing Systems (UGCS); employees shall contact the device manufacturer or their representative for operating system or hardware-related issues. Any device that is not owned by the University shall attract a fee directly or indirectly when serviced by UGCS.

User Responsibilities

It is the responsibility of users to keep their devices and its content secure. Users shall:

i. Familiarize themselves with each device and its security features so that in using it they can ensure the safety of university information.

ii. Familiarize themselves with the data categorization they work with and protect it appropriately

iii. Ensure that their devices are properly configured before accessing the University's network.
iv. Set each device to lock automatically when it is left idle.
v. Take appropriate physical security measures to ensure the device and its contents are secured and not left unattended.
vi. Use a licensed copy of all installed software including anti-malware software and keep all software up to date.
vii. Backup their work-related documents on an external storage at the end of the day.
viii. Keep primary copies of work documents on a university managed storage.
ix. Control the device's network connections by disabling automatic connection to open, unsecured Wi-Fi networks and by making risk conscious decisions before connecting.
x. Disable wireless services such as NFC, Bluetooth and wireless when they are not in use.

Data Security

To maintain the security of data, users shall:
i. Lock their devices when not in use
ii. Keep their devices operating systems and applications up to date.
iii. Enable whole disk encryption if the device supports this feature.
iv. Encrypt all University data on the device always
v. Delete any confidential University information if there is no longer a legitimate need to maintain such data on the device.
vi. Avoid accessing or storing confidential University information on a personally owned device. Use the University approved individual or departmental storage (Microsoft OneDrive)
vii. Remove all University information from the device and return it to the condition in which it was when it was first bought before they sell, exchange, or dispose of it.
viii. Immediately report the loss or theft of any device that contains University data.

Enforcement

This policy shall be enforced by the UGCS. Users who breach this policy may be subject to disciplinary and legal action by authorities of University of Ghana.

ICT PROCUREMENT POLICY

Purpose

This policy aims to provide a framework for the procurement of ICT hardware and software within the University of Ghana.

Introduction

The University of Ghana has standardized its ICT resources such as desktop software, operating systems, computer networks, computer hardware and peripherals, such as printers. (Refer to ICT Equipment Standard)

This standardization is essential as it allows the University of Ghana Computing Systems to provide a quality service with the following benefits:

i. Support engineers who are familiar with installed hardware and peripherals. As a result, improving fault finding and diagnosis;
ii. Hardware and software with a known “support state” at the time of purchase
iii. Stocked economic levels of required parts to reduce down-time;
iv. Centrally planned and coordinated installations by experienced engineers;
v. Effective planning, maintenance, upgrades, and disposal obtained from a campus-wide inventory of ICT resources
vi. Value negotiations and pricing advantages shall be obtained through volume purchasing.

This policy provides guidance on how to achieve these benefits and to ensure that the lifecycle of procuring ICT equipment’s is coordinated successfully.

Major Projects

Projects undertaken in the University of Ghana with significant investments in ICTs (Information and Communications Technology) or related equipment (hardware, software or updates to existing hardware or software) must have a representative of the UGCS on the Project steering committee who shall ensure that management of the ICT component of the project is in accordance with best practices.

Procurement Guidelines

The UGCS is the sole authority for submitting requisitions for the procurement of ICT equipment on behalf of any College, School, Unit or Department that has had approval for obtaining such equipment.

i. All ICT related resources shall be specified by the UGCS. Such resources shall not be purchased without a completed ICT Procurement Request Form signed by the user's Head of Department, Dean, or Provost.

ii. On receipt of the completed form, the UGCS shall acknowledge its receipt within eight [8] hours of receipt and proceed to process the request.

iii. The Chief IT Officer shall decide with the appropriate stakeholders, whether to approve, decline or amend the requirements for the purchase of the equipment.

iv. If equipment is declined or changed, the Chief IT Officer shall provide a brief explanation to the requesting Head of Department, Dean or Provost for the decision within twenty-four [24] hours of acknowledging receipt of the request. The request shall be deemed to have passed if no notification or explanation is provided within the twenty-four [24]-hour timeframe.

v. If the equipment is approved or changed (and accepted by the beneficiary), then UGCS shall order the equipment through the Procurement Unit.

vi. UGCS may also recommend equipment suppliers, but the Procurement Unit may change these in favour of a better price or service. The Chief IT Officer shall be notified of this change.

vii. Equipment shall only be ordered according to the Procurement Unit's procurement plan and the assigned priority. Where equipment is authorized and ordered, the UGCS shall plan to install it on delivery.

viii. All delivered equipment shall be inspected by the UGCS. The UGCS shall check for compliance with the ordered specification before equipment is setup and transported to the destination.

ix. The UGCS shall be responsible for arranging delivery of the equipment to its intended destination.

x. The UGCS shall inform the original requestor when the equipment is delivered to the UG or UGCS stores and shall plan for installation.

xi. The UGCS shall ensure that the equipment is configured appropriately and that all IT security measures are addressed.

xii. The UGCS shall ensure that all the University of Ghana's ICT guidelines, procedures, and Standard Operating Procedures (SOPs) are followed when setting up ICT resources.

xiii. For the purposes of this document, ICT resources acquired through projects, grants, donors or any such activity within the University belongs to the University of Ghana.

Non-Standard Equipment

Standardized ICT resources may not necessarily meet the needs of all users. Some situations may require specialized or customized equipment for several reasons including:

i. Specialized software which may determine the choice of hardware.

ii. Performance requirements which are peculiar to the job requirements of a user.

iii. Users whose teaching and research responsibilities require an alternative to the standard configuration.

iv. Users whose specific technical, environmental, or functional job responsibilities require an alternative to the standard configuration.

Such ICT resources shall be exceptions, and a justification of the need for such equipment shall be discussed with the UGCS. The UGCS shall procure non-standard equipment on behalf of the user once approval is received from the appropriate department. The UGCS shall make every reasonable effort to support non-standard equipment procured under such circumstances. Non-standard equipment from donors shall be evaluated by UGCS to determine its suitability for use. Equipment that is not fit for the purpose shall be disposed of appropriately.

Roles and Responsibilities

- All purchasers of computer hardware and software
  It is the responsibility of Heads of Department,Schools, and Colleges to ensure that this policy is adhered to.
- University of Ghana Computing Systems
  It is the responsibility of the UGCS to ensure that this policy is adhered to, and that ICT resources are purchased only in accordance with this policy.

Procurement Unit

It is the responsibility of the Head of Procurement to ensure that all purchases of ICT resources have been made in accordance with this policy.

Advice	**Contact**	**IP Number / email address**
Initial enquiries and advice on specifications	IT Help Desk	3000 / support@ ug.edu.gh
Approval of all ICT hardware orders and advice on standards	Deputy CITO IT Infrastructure	3120
Approval of all ICT Software orders and advice on standards	Deputy CITO IT Services	1444
Advice on order progress	Procurement Unit	2046

UG Website Policy

Purpose

University of Ghana (UG) website is a representation of the identity and culture of the University's history, research, accomplishments, and service offerings. The purpose of this document is to provide guidance on the use of the website and protect its integrity while presenting it in a user friendly and accessible manner.

Policy

Websites of Colleges, Directorates, Schools, Institutes, Units etc. of the University shall be vetted and hosted by University of Ghana Computing Systems (UGCS) to ensure compliance with this policy. Official communication of the University to the public shall always be referred to the Public Affairs Directorate (PAD) who are the official mouthpiece of the University.

Responsibilities

i. The University of Ghana Public Affairs Directorate (PAD) is responsible for the content management of the main University of Ghana website and all other social media accounts. PAD sets the standards for text, graphics, videos, and other content properties for the University website.

ii. Colleges, Schools, Departments, and Institutions are responsible for content on their websites, however, they shall conform to the directives of the PAD

iii. The University of Ghana Computing Systems (UGCS) is responsible for providing the technical framework for designing UG websites such as authoring tools, creating templates and hosting of all University of Ghana websites; providing guidance and support on a variety of web projects; ensuring that the content standards approved by the Public Affairs Directorate are adhered to

Updates and Changes

Websites shall not be updated without written authorization from the PAD and their designated appointee at the college level. Requests to update specific web pages must be submitted to UGCS via this online (link).

UGCS shall respond within two (2) working days with either notification of the completed task or a timeline for its completion. All updates shall be reviewed and verified by the PAD and their designated appointee at the college level and in some cases the Registrar's and Provost's offices, to ensure consistency with the University's mission, brand, and voice.

Style Guidelines

Style guidelines have been provided by the web planning committee and can be accessed here. Webmasters may be flexible in their presentation; however, they shall adhere to the style guidelines to ensure a common characteristic across the University's official website.

Use of seal

The University of Ghana seal may only be used on the home page and on all official pages. The seal is reserved for only the most official forms of business.

Backgrounds

Please refer to Web Standards document

Text, Headings and Body

Please refer to Web Standards document

Graphics (Photo, Video and Animated GIFs) Guidelines

Please refer to Web Standards document

Website Template

UGCS has provided official templates for creating University of Ghana webpages. This template may be customized according to the various needs of Colleges, Schools, Departments, and

Institutes. The use of the template is to ensure consistency and ease of implementation. Requests for website template shall be submitted to UGCS via this online link

Use of External Web Developers

Colleges, Schools and Units may engage external web developers to develop their website for them. All third party's developers shall comply with all the standards specified in this document.

Hosting

Web projects launched without proper consultation or approval from UGCS shall be flagged for appropriate measures and taken down.

New Web Development Projects

All new website projects requests shall be submitted to the CITO for review and approval.

Advertising and Posting

Any advertising of services or merchandise that are not related to the University of Ghana business is prohibited.

Accessibility

Regardless of disability, the University of Ghana is committed to ensuring that its website is accessible to all users. For this reason, all websites associated with the University of Ghana shall conform to the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG 2.0).

Domain Name Approval

New domain name or web server address requests shall be submitted to the UGCS for review and approval.

Exceptions

Any exceptions to this Web Policy shall be approved by the Public Affairs Directorate.

INFORMATION SECURITY POLICY

Introduction

University of Ghana acknowledges that information is the lifeblood of its very existence. Information exists in many diverse forms. Regardless of the form it takes, or how it is shared or stored, information shall always be protected appropriately. Information security is concerned with guaranteeing confidentiality, integrity, and availability (CIA). Any compromise of information security may affect the reputation and the proper functioning of the University.

This policy provides the framework for managing information security within the University.

Objectives

The objectives of this policy are to ensure that:

i. All UG's ICT resources are effectively protected against loss, misuse, or abuse.
ii. All users are aware of and comply with this policy and all other associated policies.
iii. Paper records and research data are secured and protected.
iv. Security awareness culture is intensified within the UG community.
v. Users are aware of their responsibility in handling University data.
vi. Information is discarded appropriately and in a secure manner when it is no longer relevant.

Sensitive Data

The following data are considered sensitive and confidential by the University of Ghana and shall be processed and disseminated with the appropriate guidelines that apply:

i. Information relating to a user's performance, grading, promotion, or personal and family life.
ii. Any data relating to user's health records, financial record, disability, ethnicity, sex life, trade union membership, political or religious affiliations, etc.

iii. Information relating to alumni or students' programmes of study, grades, progression, or personal and family life.
iv. Data relating to users of the University that may be used for fraud, impersonation, or identity theft, including, but not limited to, personal contact details, date of birth, salary, bank account number, national identification number etc.
v. University's contracts, proposals, policies, discussion papers, strategies etc. that may have a significant impact on any user before the decision or change is announced.
vi. Security arrangements for high profile or vulnerable visitors, students, or events. This includes passwords for access to the University network or other key systems.
vii. Exam questions before the exam takes place.
viii. Data that has the potential to seriously affect any third-party interest or the University's corporate reputation, such as an external organisation's research information.
ix. Information obtained under a confidentiality agreement where disclosure could seriously affect the University's reputation.
x. Information that, if compromised, may disadvantage the University in commercial or policy negotiations.

Policy

The University requires all its community and partners to appropriately secure information for which it is responsible, to protect such information against interruptions to its availability; failures of integrity; the consequences of breaches of confidentiality; and damage, loss, or misuse.

Responsibilities for Information Security

i. All users of UG's ICT resources have the responsibility for protecting such assets.
ii. Each user is responsible for his/her understanding of and compliance with this policy and any codes of practice.
iii. It is the responsibility of the records manager to develop procedures, give advice on good practices as well as promote

compliance with the UG records policy.

iv. Heads of Department shall ensure that their staff or students are aware of this policy.

v. Heads of Department shall implement this policy in respect of both paper and electronic records operated by their respective units and shall be responsible for ensuring authorized user are aware of and comply with the policy and associated codes of practice. Where appropriate, Heads of Department, in consultation with UGCS shall appoint for each unit a data custodian who works with data owners to ensure data security. Heads of department shall ensure adequate oversight of data security.

vi. The University of Ghana Computing Systems (UGCS) is responsible for defining an information security policy and for ensuring it is regarded by all academic and administrative units. An Information Security Governance Committee (ISGC) shall be set up and be in charge for this policy.

vii. The UG Information Technology Security Group (ITSG), in addition to its involvement in policymaking, provides relevant operational services.

viii. It is the responsibility of system owners to ensure that appropriate compliance guidance for users is always provided.

ix. There shall be an annual risk assessment on all ICT resources.

x. The Chief Information Technology Officer (CITO) shall ensure that information systems are protected and that IT security processes are run effectively.

Information Security Guidelines for All

i. Information and services in the University are categorized as unrestricted or public, internal only and confidential.

ii. All users shall safeguard the confidentiality, integrity and availability of all University information and resources.

iii. University electronic data shall always be stored in the University's approved storage space (Microsoft OneDrive).

iv. All access credentials shall be used in accordance with the appropriate guidelines.

v. Access controls for all systems shall be set at an appropriate level in accordance with the value of the assets and criticality of the system. The system owner shall authorize any changes in access permissions while access controls are revised periodically.

vi. A suitable access mechanism with security appropriate to the criticality of the system shall be used to gain access to information systems. Additional controls shall be employed to provide a stronger assurance of security when accessing critical systems.

vii. All access to high criticality services shall be logged, retained, and monitored to identify potential misuse of systems or information.

viii. Change management procedures shall be followed for all changes on all University systems.

ix. Security logs shall be managed and reviewed.

x. System clocks shall be regularly synchronized across all University ICT systems.

xi. All security incidents shall be handled as described in the Information Security Incident Management Procedure.

xii. Remote users of the University's ICT resources shall familiarize themselves with the additional risks to which they are vulnerable to and take appropriate steps to mitigate them.

xiii. ICT security training shall be given to all users and especially those involved in handling and managing internal only or confidential information and systems.

xiv. UGCS shall make available specialist advice on information security throughout the wider University community.

Retention of Data

i. Personal data shall be retained for not more than a period necessary to achieve the purpose for which the data was collected and processed.

ii. Personal data of staff and students shall, however, be in use by the University for the purposes of alumni and other resource mobilization activities of the University

iii. Student records, policy documents and publications shall be retained permanently by the University

iv. Personnel records shall be retained sixty (60) years after its creation and twenty-five (25) years after the personnel has retired.

v. Medical records shall be retained permanently by the University hospital as per local and other international best practices.

vi. Electronic records shall be retained for ten (10) years and reviewed

vii. All other records shall be retained for five (5) years after its creation, five (5) years as a closed file with its creator and five (5) years at the records centre after which the record is reviewed.

viii. The reviewing panel shall be constituted by the creator of the record, a representative of the Legal Counsel, a representative of the UGCS and the University Archivist.

Data Security

A data controller shall protect the integrity of personal data in his/ her possession through appropriate measures to prevent the loss, damage, unlawful access, or unauthorized processing of personal data.

Elevated risk personal data and sensitive business information shall be treated as confidential and protected appropriately. In the case of physical records, these shall be locked in a cabinet and access provided under the appropriate authorization. For electronic records, data shall be encrypted always with the UG appropriate encryption algorithms and stored appropriately.

Personal data shall be treated as confidential and shall not be disclosed unless required by law or in the discharge of duty.

The data controller shall take reasonable measures to identify risks posed to personal data and mitigate them accordingly

Compliance with Legislation

Staff, faculty, and students of UG have an obligation to abide by all relevant Ghanaian legislation. Of importance in this respect are the ***Cybersecurity Act 2020 (Act 1038), Electronic Transaction Act (Act 772), and Data Protection Act 2012 (Act 843).*** This policy is subject to the Data Protection Act's requirement for a formal statement of UG's security arrangements for personal data.

Risk Assessment and Security Review

i. Custodians of data shall value information they handle using a risk framework that shall be provided by the Chief Risk Officer upon approval of this policy. The risk-based approach helps to identify the value of information without compromising its integrity.

ii. UGCS shall establish effective plans to mitigate outcomes of any risk appropriately. UGCS shall periodically re-evaluate the security arrangements for its information resources.

iii. A periodic risk review of business processes and legislation is necessary to ensure an effective risk framework.

Breaches of Security

i. Any user who suspects a security breach of any information resource shall report the matter to UGCS immediately through its service desk channels.

ii. In the event of an information security breach, UGCS shall provide specific guidance on steps to follow.

iii. All physical security breaches related to ICT resources shall be reported to UGCS.

iv. UGCS shall monitor and protect ICT infrastructure and information resources to always ensure availability.

v. The University Council has the ultimate authority to take whatever action is deemed necessary to protect UG against breaches of security.

Policy Awareness and Disciplinary Procedure

i. The HRODD and the Academic Affairs Directorate shall make available this policy to all new members of staff and students. Existing users must familiarize themselves with this policy and associated procedures, codes of practice and guidelines. The failure of any user to comply with this policy may lead to disciplinary action by appropriate university disciplinary committee and, in certain circumstances, legal action against that user.

ii. Any request for information or training regarding this policy shall be addressed to UGCS Service Desk.

Supporting Policies, Procedures and Codes of Practice

i. This policy framework shall be used in conjunction with supporting guidelines, procedures and codes of practice published with it which are available on the UGCS website. Authorized users who access the UG network systems and facilities identified in this policy, shall familiarize themselves with these documents and work in accordance with them.

ii. In compliance with the ***Data Protection Act 2012,*** all personal and sensitive data shall be stored securely with adequate protection

REFERENCES

This policy document was adapted from relevant University of Ghana policy documents, national acts and ICT policies of the following institutions listed below

- University of Ghana Strategic Plan
- University of Ghana HRODD Draft Policy
- University of Ghana Records Policy
- Data Protection Act, 2012 (Act 843)
- Cybersecurity Act, 2020 (Act 1038)
- Electronic Transactions Act, 2008 (Act 772)
- NIST (National Institute of Standards and Technology) SP 800-53 rev. 5
- Blackpool and The Fylde College, Lancashire
- Chester College of Higher Education
- Murdoch University
- National University of Singapore
- Northern Caribbean University
- Oxford University
- Royal Holloway and Bedford
- Sheffield Hallam University
- Staffordshire University
- Stephenson College, Leicestershire
- The University of the South Pacific
- University of Bath
- University of Maryland
- University of Melbourne
- University of Stellenbosch, South Africa

2022, Public Affairs, University of Ghana