DIRECTORATE OF INFORMATION TECHNOLOGY SYSTEMS AND OPERATIONS

ICT AND AI POLICY

DRAFT VERSION 1.0

INTRODUCTION

The University of Environment and Sustainable Development (hereafter referred to as UESD or "the University") adopted Information and Communication Technology (ICT) as a key instrument to achieve the University's missions and vision. To this end, the University through the Directorate of Information Technology Systems and Operations (DITSO) provides and supports interactive electronic communication services and facilities such as VoIP, teleconferencing, video conferencing, electronic mail, social networking services, electronic publishing services and bulletin boards to its stakeholders. These communication services and functions are delivered over both physical and Wireless Network Infrastructure unified by Digital technologies.

The University recognizes this technological convergence and establishes a comprehensive policy framework to govern and streamline electronic communication across it ecosystem. It also clarifies the applicability of law and other University policies to electronic communication and establishes new procedures where existing ones do not specifically address issues particular to the use of electronic communication. Where there are no such issues, it refers to other University policies. This Policy may not anticipate all the new issues that might arise in electronic communication. However, the policy is time bound and subjected to amendment from time to time when necessary.

POLICY STATEMENT

This ICT and AI policy is provided to support teaching, learning, research and administrative work of the University. The data held on the network forms part of its critical assets and are subject to security breaches that may compromise confidential information and expose the University to losses and other risks. The ICT and AI Policy is subject to change from time to time and therefore users are encouraged to be aware of these changes which will be made available at the University Website. Any infringement of these regulations constitutes a disciplinary offence under the University's Statutes and Regulations. Failure to comply with any aspect of this policy will be addressed in accordance with the UESD Staff Disciplinary Policy. Abuse of these regulations may result in the user's account(s) being suspended.

For further information, contact DITSO through Intercom: 4002 or Website: https://ditso.uesd.edu.gh/ or Email: ditso@uesd.edu.gh

PURPOSE

The purpose of this guideline is to:

1. provide guidelines for the conditions of acceptance and the appropriate use of hardware, software and networking resources provided for use by academic, professional and support staff, and students at the University in carrying out their duties towards the realization of the mission and vision of the University.
2. provide mechanisms for responding to internal and external complaints about actual or perceived abuses originating from the University's computer systems and or network; protect the privacy and integrity of data stored on the University's network.
3. mitigate the risks and losses from security threats to computing and networking resources such as virus attacks and compromises to networks and systems.
4. encourage users to understand their own responsibility for protecting the University's digital resources.

AUDIENCE

These regulations apply to:

- Users (academic, professional and support staff, students and others as authorized by the University with extended access privileges). Throughout this Policy, the word 'user' will be used collectively to refer to all such individuals or groups.

CUSTODY

1. The electronic resources of the University are to be used for academic, research, consultancy or other business purposes in serving the interests of the University and its students, staff and clients during normal operations.

2. Any ICT or electronic communication address, site, number, account, or other identifier associated with the University or any unit of the University, or assigned by the University to individuals, departments, units/sections, or functions of the University, is the property of the University. However, DITSO is responsible for setting up, maintaining and keeping all IT equipment.

RESPONSIBILITIES

1. The holder of a University computer account or computer system linked to the University's ICT system is fully responsible for the actions associated with the computer account or computer system.
2. Users must ensure that they use all reasonable means to protect their equipment and (if applicable) their account details and passwords.
3. Users are responsible for University Data/Information within their domain. It is the responsibility of staff and students to inform the University when this data is lost or tampered with (including personal, academic and financial records.)

SCOPE

1. This guideline applies to all users of the University's ICT resources including staff of DITSO.
2. Users and administrators of ICT resources are responsible for making themselves familiar with the policy guidelines governing ICT resources and services in the University.

This guideline framework provides:

1. ICT governance and management of ICT services and facilities.
2. Promoting virtual teaching, learning and research, and enhancing Library services.
3. Development and use of Management Information Systems.
4. Secure use of ICT facilities.
5. Managing the University website, social media sites, internet use and email services.
6. Procurement of ICT tools and services; and
7. Any other ICT related services.

ACCEPTABLE USE

The electronic communication systems and services have been provided by the University to support the Schools, Directorates, Centres, Departments, Units and Sections in performing their academic work. The use of these facilities constitutes acceptance of this policy and is subject to the following limitations which are necessary for their reliable operations:

1. Users must comply with all applicable ICT policy guidelines.
2. The electronic resources should be used for the purposes for which they are intended.
3. Users must respect the rights, privacy and property of others.
4. Users must adhere to the confidentiality rules governing the use of passwords and account details, which must not be shared.
5. Temporary passwords provided by IT Support staff to users must be changed immediately following a successful login.
6. Whilst the University network is being used to access other networks, any abuses against such networks will be regarded as an unacceptable use of the University network.

PERSONAL USE

The University network, computing facilities and materials may be used for incidental personal purposes provided that:

1. The purposes are of a private nature, not for financial gain and does not contravene any other policy of the University.
2. Such use does not cause noticeable or unavoidable cost to the University.
3. Such use does not inappropriately interfere with the official business of the University.

UNACCEPTABLE USE

1. The University network, computing facilities and materials must not be provided to individual consumers or organizations outside the University except where such services support the mission of the University or are in the commercial interest of the University and permission has been granted by Management of the University.
2. The University adopts a policy of cooperation with copyright holders and law enforcement bodies and may suspend or remove content published online while investigating claims from such bodies.
3. The University will from time-to-time act to suspend or remove content from websites which jeopardize the University's reputation or brand. In the case of content published on the University's websites, this should be reported through Intercom: 4002 or Email: ditso@uesd.edu.gh
4. Any misuse of the University network facilities may be seen as a breach of the University's Code of Conduct and may lead to disciplinary action.
5. The University network may not be used for the creation, dissemination, storage and display of:

    a. obscene or pornographic material.

    b. racial and discriminatory literature.

    c. racial and discriminatory material that promote criminal activities.

d. defamatory materials or materials that are likely to cause offence to others.

e. any data that is illegal including, but not limited to, Statutes and Regulations of the University.

6. Downloading, storage and disseminating copyright materials including software and all forms of electronic data without the permission of the holder of the copyright or under the terms of the licenses held by the University.

7. Any activities which do not conform to applicable laws and other University guidelines and policies regarding the protection of intellectual property and data.

8. Deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting data belonging to other users.

9. Using the network for commercial work for outside bodies without explicit permission from the University Management.

10. Use of a username and password belonging to another user.

11. Attempts to falsify identity or to pretend to have a different affiliation with the University when sending email from a university computer.

12. Attempts to crack, capture passwords or decode encrypted data.

13. Any other use that may bring the name of the University into disrepute or expose the University to the risk of litigation.

14. Intentional or reckless creation, execution, forwarding or introduction of any viruses, that could hinder the performance of the University network.

15. Attempts to hack whether this results in corruption or loss of data.

16. Connecting any computer device to the University network in disregard of security standards established by DITSO on behalf of the University.

PROCUREMENT, MAINTENANCE & DISPOSAL GUIDELINES

These guidelines provide information for improved asset management, better control over ICT expenditure and the implementation of acceptable standards for ICT equipment, suppliers and services. The rules and regulations governing procurement of goods and services for the Republic of Ghana which are applied by the University shall form the basis of these policy statements. DITSO shall assist the Schools, Directorates, Centres, Departments, Sections and Units with the preparation of technical specifications for the purpose of procuring ICT equipment and services. It shall also assist the Procurement Unit to identify reputable companies or registered providers to reduce any delay in the procurement process.

1.1 Scope

These guidelines apply to all UESD employees and authorized representatives and covers all expenditure, regardless of funding sources, and contractual arrangements which the University makes with ICT suppliers, consultants, contractors and donors.

Table 1.1. Definitions of Terms

ICT Equipment	This covers all servers, desktops, laptops, printers, network equipment, smart-phones, other mobile devices and peripherals and any other related ICT equip-ment.
Primary User	An individual in whose office the computer is installed and is primarily used by him/her, is "primary" user. If a computer has multiple users, none of whom are considered the "primary" users, the department Head must arrange and make a person responsible for compliance.
End User Computer Systems	Apart from the client PCs used by the users, the University will consider servers not directly administered by DITSO as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems that are acting as servers which provide services to other users on the Intranet/Internet though registered with DITSO, are still considered under this policy as "end-users" computers.
Software	This covers all computer applications developed by DITSO, including procured software and outsourced software services.
Services	This covers all contractual arrangements with ICT consultants and contractors, ICT recruitment companies, ICT training companies and outsourced ICT services.
Procurement Unit	DITSO shall work with the Procurement Unit to ensure value for money is achieved in terms of products, service quality and cost for all ICT expenditure as well as compliance with relevant legal provisions.
Procurement	All ICT equipment and service procurement must be processed through DITSO using approved suppliers and complying with any defined ICT standards applicable at the time. Any ICT equipment and service procurement exercise or contract must also comply with this Policy and guidelines.
Approved Suppliers	A schedule of approved suppliers for all defined ICT equipment, software or services will be created and maintained by the Procurement Unit in conjunction with DITSO. The University procurement procedures shall be followed.
Non-Approved Suppliers	If there is a genuine requirement to purchase ICT equipment or service from non-approved suppliers (e.g. for specialized ICT equipment not available from existing approved suppliers) a New Supplier request form detailing the rationale must be submitted to and approved by the Head of Procurement, prior to ordering.
ICT Standards	A schedule of standard ICT equipment, software and services will be created and maintained by DITSO. This list will include entry level, standard and advanced specification options for many of the categories of ICT equipment. Where standards are in place for ICT equipment or services these must be adhered to when requesting a purchase. Purchase of alternative make or model of equipment or software package with similar functionality is not acceptable where university standards have been defined and published. Applications for adding new equipment or services to the approved list should be made in writing to the Director, DITSO.
Non-Standard ICT Equipment & Services	If there is a genuine requirement to purchase ICT equipment or services outside the published standard list (e.g. for Enabling Support desktop equipment or software where no standards currently exist) approval must be sought from management before ordering.

Compliance	Compliance with this policy will allow the University to negotiate better discounts and establish higher levels of service from fewer suppliers, resulting in lower administrative overheads. Standardization of ICT equipment and services will also allow improvements in service through a reduction in compatibility issues, fewer varieties of hardware and software to support, improved hardware refresh and maintenance programmes and faster turnaround for new equipment or service requests. Failure to comply with any aspect of this policy will be dealt with in accordance with the UESD Staff Disciplinary Policy.

1.2 Policy Guidelines for Acquisition of Equipment and Services

The following statements shall govern the procurement of ICT equipment and services:

1. The Unit requesting the equipment must do so in conjunction with DITSO. The University procurement procedures shall be followed.

2. All ICT equipment and services procurement must be processed through DITSO using approved suppliers and complying with any defined ICT standards applicable at the time. All ICT equipment and services procurement exercises or contracts must also comply with these guidelines.

3. DITSO shall work with the Procurement Unit to ensure value for money is achieved in terms of products and services quality and cost for all ICT expenditure as well as compliance with relevant legal provisions. If there is a genuine requirement to purchase ICT equipment or services from non-approved suppliers (e.g. for specialized ICT equipment not available from existing approved suppliers) a New Supplier request form detailing the rationale must be submitted to and approved by the Head of Procurement, prior to ordering.

4. A schedule of standard ICT equipment, software and services will be created and maintained by DITSO. This list will include entry level, standard and advanced specification options for many of the categories of ICT equipment. Where standards are in place for ICT equipment or services these must be adhered to when requesting for a purchase. Purchase of alternative make or model of equipment or software package with similar functionality is not acceptable where University standards have been defined and published. Applications for adding new equipment or services to the approved list should be made in writing to the Director, DITSO.

5. If there is a genuine requirement to purchase ICT equipment or services outside the published standard list (e.g. for Enabling Support desktop equipment or software where no standards currently exist) approval must be sought from management before ordering.

6. Compliance with this guideline will enable the University to negotiate better discounts and establish higher service levels with fewer suppliers, leading to reduced administrative overheads.

7. Standardizing ICT equipment and services will enhance service delivery by minimizing compatibility issues, reducing hardware and software variations, improving hardware refresh and maintenance programs, and ensuring a faster turnaround for new equipment or service requests.

8. Identification of the needs and the justification for procurement of ICT equipment and services shall be done by or in consultation with DITSO.

9. DITSO shall develop the technical specifications and shall ensure the beneficiary department/unit/ section use up-to-date and state-of-the-art technology.
10. This procurement policy shall comply with all financial regulations of the University.
11. DITSO shall undertake a periodic inventory of all ICT equipment and services procured by the University.
12. DITSO shall check the delivery schedule, examine compliance with technical specifications and perform tests on equipment in accordance with the contract awarded to the supplier.

1.3 Warranty & Annual Maintenance Contract

All devices (Computers, Servers, MFP Printers and Accessories) purchased by the Directorate on behalf of the University shall preferably be with a 2-year on-site comprehensive warranty. After the expiry of warranty, all devices shall be under Annual Maintenance Contract (AMC). Such maintenance shall include comprehensive on-site maintenance of Desktops, Servers and MFP Printers, OS reinstallation and checking virus related problems. Replacement of defective parts will be at the vendor's cost with original spares of the brand/make of the devices within ten (10) working day.

1.4 Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT Staff must perform the tasks before and after normal business hours. Tasks that are deemed "emergency support," as determined by the Director or his/her designee, can be performed at any time.

1.5 Manufacturer Support Contracts

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the UESD must purchase a maintenance plan, support agreement, or software subscription that will allow the UESD to receive updates to the software and/or firmware for a specified period. The plan must meet the following minimum requirements: Hardware: The arrangement must allow for repair/replacement of the device within an acceptable period, as determined by the CIO or their designee, as well as firmware or embedded software updates. Software: The arrangement must allow for updates, upgrades, and hotfixes for a specified period.

1.6 Power Connection to Computers and Peripherals

All the computers and peripherals shall be connected to the electrical point strictly through UPS systems. Power supply to UPS shall never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems shall be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

1.7 File and Print Sharing Facilities

File and print sharing facilities on the computer over the network shall be installed only when it is absolutely required. When files are shared through the network, they shall be protected with password and with read only access rules.

1.8 Policy Guidelines for Maintenance

1. For all the computers that have been purchased by the university centrally and distributed by DITSO, IT Support Services Unit (hardware technician) will attend to the complaints related to any maintenance related problems.
2. All ICT equipment shall be serviced regularly every quarter.
3. DITSO shall carry out preventive maintenance on all computers and accessories.
4. Outsourced Maintenance services shall be carried out as per the agreed vendor Service Level Agreement for Critical Equipment.
5. Equipment such as Printers, Cooling and Power systems shall be placed on maintenance contracts where necessary.

1.9 Policy Guidelines for Movement of Equipment

Computer systems may be moved from one location to another with prior written approval from DITSO, as the Directorate maintains a record of computer identification names and corresponding IP addresses. Such computer identification names shall follow the convention that comprises department name abbreviation, computer type and number. As and when any deviation (from the list maintained by the Directorate) is found for any computer system, network connection would be disabled and the same would be communicated to the user by email/phone, if the user is identified. When the end user meets the compliance and informs the Directorate in writing/by email, connection will be restored.

1. No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location, without the explicit permission of the Directors, DoF, DPDEM and DITSO.
2. No equipment other than designated portable devices to be used outside the University campus shall be taken out without the express permission of the Directors, DoF, DPDEM and DITSO or their representatives.
3. For permission to be granted, the necessary forms detailing the purpose of the movement of the equipment and equipment details must be provided by the user and countersigned by the appropriate head of the user.

1.10 Policy Guidelines for Replacement/Disposal of Equipment and Services

The life cycle of ICT equipment and services shall depend on their functionality as detailed in (Table 1.9a) and performance:

1. However, the average life span of ICT equipment shall be five (5) years.
2. For software, the average life span shall be dependent on the release of new versions in accordance with the software maintenance agreement.
3. The frequently changing IT environment means that ICT equipment periodically becomes obsolete or reaches the end of its useful life. DITSO shall ensure that the data stored on such computers are securely removed prior to their disposal.
4. No IT equipment (including portable devices) may be disposed off by entity other than by DITSO via the processes set out in this policy. Users with equipment which needs to be disposed of shall contact DITSO to ensure safe disposal of the equipment.
5. All IT equipment must be disposed of in accordance with the University's Waste Management Policy.
6. Prior to the disposal of computer equipment, all personal and sensitive data must be securely destroyed by a method appropriate to the risk associated with the sensitivity of data and the equipment on which it is stored as set out in Table 1.2 below.
7. All other data and any software licensed to the University shall be removed prior to the equipment leaving the possession of the University.
8. If IT equipment is disposed of by third party contractors on behalf of the University, they must adhere to the relevant standards and provide the relevant certificates of destruction and copies of waste consignment notes.

Table 1.2. Check list for replacement/disposal of equipment

Item	Data/Use	Risk	Data Destruction Method	Reasons
PCs & Laptops	Standard office use on managed desktop and student PCs	Low	Overwriting drive multiple times	• Low risk of relevant data being on PC in the first place • Efficient in terms of volume of equipment, staff time, physical space
	Regularly used for processing personal data or sensitive personal data e.g. HR, Finance, Senior Managers	Medium	Overwriting drive multiple times	• Relevant data is likely to be present, therefore need for security outweighs operational efforts required • Will ensure data is effectively not recoverable • Data on laptops should be encrypted so if recovered will still be encrypted
	Used for processing non-personal confidential or commercially sensitive data	Medium	Overwriting drive multiple times	• Relevant data is likely to be present, therefore need for security outweighs operational efforts required • Will ensure data is effectively not recoverable • Data on laptops should be encrypted
	Research projects involving large amounts of sensitive personal data where data has been stored locally but not encrypted	High	Physically destroy	• Impact of data loss could lead to court action, severe reputational damage and loss of future research income
Servers	Storage of personal data, sensitive personal data and confidentiality of commercially sensitive data	High	Physically destroy	• Large volumes of data. • Mix of personal, sensitive personal, confidential, commercially sensitive data. • Disks are not in practice resold but are reused in other University systems until they fail or become obsolete.

Other Portable devices	CDs, USB sticks (pendrives),floppydisks,memory cards, tapes	Medium	Physically destroy	• Simple and most secure option. • With CD-Rs there is no option to overwrite. • For CD-R should be undertaken as soon as the data is no longer needed to be stored in that way. • For other removable media should be undertaken when the storage device is no longer needed.
	Larger USB drives, and external hard disks.	Medium	Overwriting drive multiple times	• Relevant data is likely to be present, therefore need for security outweighs operational efforts required • Will ensure data is effectively not recoverable.

1.11 Non-Compliance

Faculty members, staff, and students not complying with this IT equipment procurement, maintenance & disposal policy may leave themselves and others at risk of network-related problems which could result in damaged or lost files, inoperable computers resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be. The Services Unit upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone. The individual user should follow-up the notification to be certain that his/her computer gains necessary compliance. The Services Unit will provide guidance as needed for the individual to gain compliance.

2.0 NETWORK GUIDLINES

Network connectivity for the University is provided through an authenticated network access connection governed under the University IT Policy. The Network, Systems and Telecommunication Unit is responsible for the ongoing maintenance and support of the Network, exclusively for local applications. Problems within the University's network should be reported to the network team.

2.1 IP Address Allocation

Any computer (PC/Server) and peripherals that will be connected to the University network, should have an IP address assigned statically or dynamically by the System/Network Administrator. Following a systematic approach, the range of IP addresses that will be allocated to each device is decided. So, as and when a new computer/device is installed or connected to the network an IP address would be allocated only from that Address pool.

An IP address allocated for a particular computer system or device should not be used on any other computer/device even if that other computer/device belongs to the same individual and will be connected to the same port. IP addresses are given to computers but not to the ports.

2.2 DHCP and Proxy Configuration

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch and distributing IP addresses (public or private) should strictly be avoided, as it is considered an absolute violation of the IP address allocation policy of the University.

Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by the Network Systems and Telecommunication Unit. The configuration of any computer with an additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration. Non-compliance with the IP address allocation policy will result in disconnecting the port from which such a computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned user.

2.3 Network Services

Individuals connecting to the University's network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server that is installed and provided by DITSO only after explicit written permission of the Directorate and after meeting the requirements of the University IT policy for running such services.

Non-compliance with this policy is a direct violation of the University's IT policy and will result in termination of their connection to the Network. DITSO takes no responsibility for the content of machines connected to the Network, regardless of those machines being the University's or personal property. DITSO will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance. Access to remote networks using the University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at the Directorate. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

2.4 Broadband Connections

Computer systems that are part of the University's campus-wide network, whether University's property or personal property, should not be used for broadband connections, as it violates the University's security by bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address assigned to that computer system.

2.5 Wireless Local Area Network

DITSO has overall responsibility for the University's data communications infrastructure. The IT directorate will therefore be responsible for the deployment, management and support of all wireless local area networks that serve common flexible access areas and all areas where a connection to the University's campus network is required. DITSO and other authorized providers may only deploy wireless LANs that conform to this Policy and all other University Information Technology Policies. Only hardware and software conforming to wireless standards approved by this Policy shall be used in wireless LAN deployments.

All wireless LAN deployments must be registered with DITSO who will periodically check the deployment for compliance with this policy. If interference problems occur between wireless LAN deployments, then DITSO will arbitrate to provide an acceptable resolution. Network access to Schools, Departments, or Units must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted to operate on the wireless local area networks.

2.6 Network Cable Connection

UESD provides a comprehensive data communications infrastructure underpinning the important role IT plays in the University's teaching, research and administrative functions. This infrastructure supports a wide range of services via a high bandwidth campus backbone that connects standards-based Local Area Networks (LANs) in all UESD premises. A centralized model for infrastructure management and support has been adopted as this provides several benefits with respect to quality, consistency, reliability, conformance, security and on-going development.

This guideline covers the connection of all equipment to the University's centrally managed campus network and building Local Area Networks. It also covers the indirect connection of equipment to the University's campus network via remote access servers. DITSO is responsible for the data communications infrastructure, in terms of:

1. Backbone fibre optic cabling.
2. Building premises distribution schemes (UTP flood wiring).
3. Backbone and Building LAN Routers.
4. Routing services.
5. Building LANs - Ethernet Switches.
6. IP address and name space and the associated support services, including:
    a. Network management/maintenance,
    b. Security, DNS,
    c. E-mail relays.

DITSO is therefore the logical entity to co-ordinate, manage and support all connections to the campus network and ensure compliance with this policy. The UESD data communications infrastructure is designed to support the teaching, research and administrative functions of the University. All Departments and Units have the right to connect to the campus network and gain access to the University's IT resources. Equipment can only be connected to the campus network if it meets the technology standards and all regulatory standards with respect to electrical and environmental safety standards. Some network connection points shall be provided to support the following equipment types:

1. User workstations including open access workstations.
2. Staff/student at selected flexible access locations.
3. Networked printers and photocopiers.
4. Telephony equipment (VoIP).
5. Video Conferencing equipment.
6. Specialized equipment e.g. imaging, scanners, process control systems.

This policy forbids Schools, Directors and Departments and directorates, users or other groups from extending centrally provided network connection points in an ad-hoc manner or connecting equipment or installing software that could be used to monitor or record network traffic, or still or moving images of the surrounding area without proper authorization from DITSO. It is therefore a breach of this policy to connect any of the following equipment or services to a network connection point without authorization:

1. Ethernet Switches or Bridges.
2. Routers.
3. Firewalls.
4. Proxy servers.
5. Access gateways include VPN concentrators and Remote Access Servers.
6. Wireless LAN access points.
7. Network cameras, including web cams that do not comply with the University's CCTV

policy.

8. Any equipment configured in promiscuous mode for the purpose of monitoring or recording network traffic not specifically addressed to that equipment e.g. traffic with a source or destination MAC address other than the Unicast address of the equipment.
9. Installing software on workstations or servers would enable unauthorized monitoring of network traffic.

2.7 Network Security

2.7.1 Purpose

The purpose of this guideline is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the UESD's comprehensive set of security policies. However, this policy purposely avoids being overly specific to provide some latitude in implementation and management strategies.

2.7.2 Scope

This guideline covers all IT systems and devices that comprise the UESD network or that are otherwise controlled by UESD. This guidelines on network security also covers systems administered by DITSO.

2.7.3 Network Device Passwords

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

2.7.4 Password Construction

The following statements apply to the construction of passwords for network devices:

1. Passwords must have at least 12 characters.
2. Passwords must comprise a mix of letters, numbers and special characters (punctuation marks and symbols).
3. Passwords must not comprise of, or otherwise utilize, words that can be found in a dictionary.
4. Passwords must not comprise an obvious keyboard sequence (i.e., qwerty).
5. Passwords must not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

2.7.5 Failed Logons

Repeated log-on failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. DITSO will lock accounts after five (5) failed log-ons to protect against account guessing. When log-on failures occur the error message transmitted to the user shall not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

2.7.6 Change Requirements

Passwords must be changed according to these Password Policy guidelines. Additionally, the following requirements apply to changing network device passwords:

1. If any network device's password is suspected to have been compromised, all network device passwords must be changed immediately.
2. If a network staff or system administrator leaves UESD, all passwords to which the administrator could have had access shall be changed immediately. This statement also applies to any other staff, consultant or contractor who has access to administrative passwords.
3. Vendor default passwords must be changed when new devices are put into service.

2.7.7 Password Policy Enforcement

Wherever passwords are used, an application must be implemented that enforces the UESD's password policies on construction, changes, re-use, lockout, etc.

2.7.8 Administrative Password Guidelines

As a rule, administrative (also known as 'root') access to systems shall be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network and its security. Additionally, administrative access to network devices shall be logged.

2.7.9 Logging

The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail the UESD's requirements for logging and log review.

2.7.9.1 Application Servers

Logs from application servers are of interest since these servers often allow connections from a lot of internal and/or external sources. These devices are often integral to smooth business operations. Examples: Web, email, and database servers.

Requirements:

1. At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary.
2. No passwords should be contained in logs.

2.7.9.2 Network Devices

Logs from network devices are of interest since these devices control all network traffic and can have a huge impact on the UESD's security. Examples: Firewalls, network switches, routers.

Requirements:

1. At a minimum, logging of errors, faults, and login failures are required. Additional logging is encouraged as deemed necessary.
2. No passwords should be contained in logs.

2.7.9.3 Critical Devices

Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any case where this occurs, this section shall supersede. Examples: File servers, lab machines, systems storing intellectual property.

Requirements:

1. At a minimum, logging of errors, faults, and login failures is required.
2. Additional logging is encouraged as deemed necessary.
3. No passwords should be contained in logs

2.7.9.4 Log Management

While logging is important to the UESD's network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, DITSO shall implement and keep the log management register.

2.7.9.5 Log Review

Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events. Also, DITSO shall manually review the logs as frequently as reasonable.

2.7.9.6 Log Retention

Logs will be retained for a minimum of 30 days. Unless otherwise determined by the Director, DITSO or his/her designee, Logs shall be considered operational data.

2.7.10 Firewalls

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks shall be separated from the UESD network through
the use of a firewall.

2.7.10.1 Configuration

The following statements apply to the UESD's implementation of firewall technology:

1. Firewalls must provide secure administrative access (using encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
2. No unnecessary services or applications should be enabled on firewalls. DITSO uses 'hardened' systems for firewall platforms, or devices.
3. Clocks on firewalls must be synchronized with UESD's other networking hardware using NTP or other means. Among other benefits, this will aid in problem resolution and security incident investigation.
4. The firewall ruleset must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
5. For its own protection, the firewall ruleset must include a "stealth rule," which forbids connections to the firewall itself.

The firewall must log dropped or rejected packets.

2.7.10.2 Outbound Traffic Filtering

Firewalls are often configured to block only inbound connections from external sources however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."
Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised. This will also prevent remote desktops from accessing the internal network. If filtering is deemed possible, only the following known 'good' services should be permitted outbound from the network: 21, 22, 23, 25, 53, 80, 110, 443, and 995.

2.7.10.3 Networking Hardware

Networking hardware, such as routers, switches and access points, shall be implemented in a consistent manner. The following statements apply to the UESD's implementation of networking hardware:

1. Networking hardware shall provide secure administrative access (using encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
2. Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
3. DITSO shall use switches to create VLANs to separate networks where possible.
4. Access control lists shall be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.
5. Unused services and ports shall be disabled on networking hardware.
6. Access to administrative ports on networking hardware shall be restricted to known management hosts and otherwise blocked with a firewall or access control list.

2.7.10.4 Network Servers

Servers typically accept connections from several sources, both internal and external. As a rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to UESD network servers:

1. Unnecessary files, services, and ports should be removed or blocked. DITSO shall follow best practices for hardening Windows OS for Windows servers.
2. Network servers, even those meant to accept public connections, shall be protected by a firewall or access control list.
3. DITSO shall develop standard installation process for UESD network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.
4. Clocks on network servers should be synchronized with the UESD's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

2.7.10.5 Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that IDS alerts about suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically act when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic. UESD requires the use of both an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) on critical or high-risk network segments. DITSO shall implement procedures to review and act on the alerts expediently. For the IPS, DITSO shall implement procedures that shall provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic. The IPS shall be audited and documented according to the standards detailed in the "Firewalls" section of this document.

2.7.10.6 Security Testing

Security testing, also known as vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the UESD's network security. Security testing can be provided by IT Staff members but is often more effective when performed by a third party with no connection to the UESD's day-to-day Information Technology activities. The following sections detail the UESD's requirements for security testing.

1. Internal Security Testing: Internal security testing does not necessarily refer to testing the internal network, but rather testing performed by members of the UESD's IT team. Internal testing does not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network. Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with the permission of the Director or their designee. Internal testing should have no measurable negative impact on the UESD's systems or network performance.
2. External Security Testing: External security testing, which is tested by a third-party entity, is an excellent way to audit the UESD's security controls. The Director or his/

her designee must determine to what extent this testing should be performed, and what systems/applications it should cover. External testing must not negatively affect network performance during business hours or network security at any time. As a rule, "penetration testing," which is the active exploitation of UESD vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact UESD systems or data.

2.7.10.7 Disposal of Information Technology Assets

IT assets, such as network servers and routers, contain sensitive data about network communications. When UESD assets are decommissioned, the following guidelines shall be followed:

1. Any asset tags or stickers that identify the UESD must be removed before disposal.
2. Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.

Data wiping technology, which meets or exceeds the Data Protection Act 2012, (Act, 843) of Ghana must be used on any hard drives prior to disposal. Simply reformatting a drive or erasing data does not make the data unrecoverable. If the data wiping technology is not possible, the device's data storage mechanism (such as its hard drive or solid-state memory) must be destroyed.

2.7.10.8 Network Compartmentalization

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, UESD will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. UESD network requires the following about network compartmentalization:

1. Higher Risk Networks:
    a. Examples: Guest network, wireless network
    b. Requirements: Segmentation of higher risk networks from the UESD's internal network is required and must be enforced with a firewall or router that provides access controls.
2. Externally Accessible Systems
    a. Examples: Email servers, web servers.
    b. Requirements: Segmentation of externally accessible systems from the UESD's internal network is required and must be enforced with a firewall or router that provides access controls.
3. Internal Networks
    a. Examples: Finance, Human Resources, Student Records
    b. Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access

2.7.10.9 Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that UESD's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable. At a minimum, network documentation must include:

1. Network diagram(s).
2. System configurations.
3. Firewall ruleset.
4. IP Addresses.
5. Access Control Lists.

UESD requires that network documentation is performed and updated on a yearly basis.

2.7.10.10 Minimum Configuration for Access

Any system, including but not limited to, workstations, tablets, notebooks, and servers, connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, antivirus software must be updated, as well as other critical software, to the latest versions before accessing the network. UESD IT may require that additional anti-malware and/or other security software be installed on computers that access the UESD network. This software will be provided by the DITSO with instructions as to the installation.

2.7.10.11 Change Management

Documenting changes to network devices is good management practice and can help speed resolution in the event of an incident. The IT Staff should make a reasonable effort to document hardware and/or configuration changes to network devices in a "change log." If possible, network devices should bear a sticker or tag indicating essential information, such as the device name, IP address, Mac address, asset information, and any additional data that may be helpful, such as information about cabling.

2.7.10.12 Suspected Security Incidents

When a security incident is suspected that it may impact a network device, the IT Staff should refer to the UESD's Incident Response policy for guidance. (Check if there is an existing doc on this).

2.7.10.13 Redundancy

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. UESD wishes to provide the Director with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and shall include some or all the following:

1. Hard drive redundancy, such as mirroring or RAID.
2. Server level redundancy, such as clustering or high availability.
3. Component level redundancy, such as redundant power supplies or redundant NICs.
4. Keeping hot or cold spares onsite.

2.7.10.14 Security Guideline Compliance

It is UESD's intention to comply with this guideline not just on paper but in its everyday processes as well. With that goal in mind UESD requires the following:

1. Security Program Manager: An employee of DITSO must be designated as a manager for the UESD's security program. He or she will be responsible for the UESD's compliance with this security policy and any applicable security regulations. This employee must be responsible for

    a. the initial implementation of the security guidelines

    b. ensuring that the policies are disseminated to employees.

    c. training and retraining of employees on the UESD's information security program (as detailed below).

    d. any ongoing testing or analysis of the UESD's security in compliance with this policy.

    e. updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

2. Security Training: A training program must be implemented that will detail the UESD's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually.

3. Security Policy Review: UESD's security policies must be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident, or a material change to the UESD's security policies. As part of this evaluation the UESD must review:
4. Any applicable regulations for changes that would affect the UESD's compliance, or the effectiveness of any security controls deployed.
5. If the UESD's deployed security controls are still capable of performing their intended functions.
6. If technology or other changes may influence the UESD's security strategy.
7. If any changes need to be made to accommodate future IT security needs.

2.7.10.15 Applicability of Other Policies

This document is part of the UESD's cohesive set of security policies. Other policies may apply
to the topics covered in this document and as such the applicable policies should be

3.0 BACKUP GUIDELINE

3.1. Definition

The backup guideline for UESD clarifies specific procedures, policies, and responsibilities, including a well-defined schedule for performing backups, ensuring a more stable process. It also identifies any superseding procedures or policies that already exist, such as contingency plans. As a rule of thumb, files created by UESD users are the type of files that should be backed up. The goals of this backup policy is as follows:

1. to safeguard the information assets of UESD Community.
2. to prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.
3. to permit timely restoration of information and business processes should such events occur.
4. to manage and secure backup & restoration processes and the media employed within these processes.

3.2 Backup Window

DITSO maintains the following type of backup profiles:

1. Standard Backup:
    a. The standard backup is provided for most centralized University computer systems.
    b. The backup should be full, differential or incremental. The frequency of backup should be daily, weekly or monthly and is dependent upon the application. The retention of these backups should vary from 1 week up to 2 months.
    c. For some applications backup should be performed on a day and time agreed upon by the organizational unit (OU) and application owner.
2. Critical System Backup:
    a. Certain enterprise-wide systems are deemed critical to university operations and dictate longer retention periods from 6 months up to 1 year.
    b. The type, frequency and retention period are different for different applications.
    c. Prior to a major upgrade of a production system, database, or application, a full system backup is performed and retained for 6 months.

d. Special Request Backup: Some departments or applications may require an exception to the standard backup retention periods mentioned above. Exceptions are permitted but must be fully documented.

3.3 Responsibility

DITSO is responsible for backing up data that is stored in central systems and databases. Data residing on individual workstation hard drives is the responsibility of the user to backup. Furthermore, the systems that fall under this category might include development or test systems that do not contain important business or academic data. Students, faculty, staff and third parties who store data on university equipment are responsible for ensuring the data is stored in a way that will ensure it is properly backed up. However, most systems that are centrally managed by DITSO shall be backed up on one of the scheduled periods listed above.

3.4 Data Backed up

There are mainly three types of backups namely Full backup, differential backup, and incremental backup. Data backed up is a copy or archive of the important information stored on users' devices such as a computer, phone, or tablet, and it's used to restore that original information in the event of data loss. Student records, financial transaction records and human resource records of UESD shall be backed up daily. It may seem unnecessary since most transaction providers offer tracking and archiving, but it's always best to have personal copies, just in case.

3.5 Verification

On a periodic basis, logged information generated from each backup job will be reviewed for the following purposes:

1. to check for and correct errors.
2. to monitor duration of the backup job.
3. to optimize backup performance where possible.

DITSO shall identify problems and take corrective actions to reduce any risks associated with failed backups. Test restores from backup tapes for each system will be performed. Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly. DITSO shall maintain records demonstrating the review of logs and test restores to demonstrate compliance with this policy for auditing purposes.

3.6 Backup Media

Media shall be clearly labelled and logs will be maintained identifying the location and content of backup media. Backup images on assigned media will be tracked throughout the retention period defined for each image. When all images on the backup media have expired, the media will be re-incorporated amongst unassigned (available) media until reused. DITSO will retire & dispose of media periodically according to the recommended lifetime defined for the backup media utilized, to avoid media failures.

3.7 Storage, Access, and Security

All backup media shall be stored in a secured area that is accessible only to designated UESD staff or employees of the contracted secure off-site media vaulting vendor used by DITSO. Backup media will be stored in a physically secured, fireproof place when not in use. During transport or changes of media, media will not be left unattended.

3.8 Retirement and Disposal of Media

Prior to retirement and disposal, DITSO shall ensure that:

1. the media no longer contains active backup images or any active backup images have been copied to other media.
2. the media's current or former contents cannot be read or recovered by an unauthorized party.
3. all backup media are physically destroyed prior to disposal.

3.9 Back-Up Documentation

Essential documentation will be maintained for orderly and efficient data backup and restoration. The person in charge of data backup shall fully document the following items for each generated data backup as detailed in the table below.

Table 3.1. Data backup check list

SN (To be provided at the time of execution)	**Action Item**	**Action**
	Date of Data backup	
	Type of Data backup (Incremental, differential, full)	
	Number of Generations	
	Responsibility for data backup	
	Extent of data backup (Files/Directories)	
	Data media on which the operational data are	
	Data media on which the backup data are stored	
	Data backup hardware and software (with version number)	
	Storage location of backup copies	

3.10 Back-Up Retention Period

Unless a system supporting an application or business function requires a custom retention period, DITSO shall maintain full and incremental backups. Backup tapes for the current weekly backup period will be stored within DITSO for purposes of current backups and restores. Tapes representing backups from the former weekly backup period will be stored within a secured, fireproof place until such time as the backup images stored on these tapes expires and the tapes are re-used or destroyed.

After a successful backup, it will be stored in a secured, off-site media vaulting location for

an appropriate period for disaster recovery purposes. This will ensure that no more than one week of information would be lost in the event of a disaster in which campus systems and backup images are destroyed. After the period of six months has elapsed, the tapes may 'optionally' be returned to DITSO and re-used or destroyed.

3.11 Data Restoration and Disaster Recovery Considerations

As soon as it is practical and safe post-disaster, DITSO shall:

1. Restore existing systems to working order or obtain comparable systems in support of defined business processes and application software.
2. Restore the backup system according to documented configuration to restore server systems.
3. Obtain all necessary backup media to restore server computing systems
4. Restore server computing systems according to the priority of systems and processes as outlined for restoration and recovery in the Disaster Recovery plan (see 7.0).

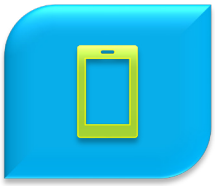
3.12 Backup Archives

DITSO shall identify data that is no longer active and move it out of production/live systems into long-term storage systems. Archival data is stored so that at any time it can be brought back into service. The primary benefits of archiving data for the University are:

1. Reduced cost data is typically stored on low performance, high-capacity media with lower associated maintenance and operation costs.

    2. Better backup and restore performance archiving, remove data from backups, reduce their size and eliminate restoration of unnecessary files.

4.0 BYOD GUIDELINE



This provides guidelines for using personally owned devices and related software for corporate use.

4.1 Applicability

The BYOD guideline applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the Director, DITSO or a designated representative. Furthermore, based on the amount of personally identifiable information (PII) employees work with, management reserves the right to determine which employee(s) can use personally owned devices and which cannot.

4.2 General Guideline

UESD recognizes that personally owned equipment can play a valuable role in the convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by the University for corporate use:

1. Desktop computers
2. Laptop computers
3. Tablets
4. Personal digital assistants (PDAs)
5. Smart phones
6. Portable music players

4.3 Device Registration

All personally owned devices must be registered with DITSO.

4.4 End-User Support

As a rule, users of personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

DITSO will support personally owned devices as follows:

1. The user will be required to allow DITSO to load security software on each device.
2. The user will be required to allow DITSO to install remote wiping software on each device.
3. Upon request, the DITSO shall install the necessary synchronization software to the user's desktop or notebook computer.

4.5 Device Security

The user should follow good security practices including:

1. Password-protect all personally owned devices
2. Do not leave personally owned devices unattended

4.6 Release of Liability and Disclaimer to Users

1. DITSO hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability.
2. In the case of litigation, may take and confiscate a user's personally owned device at any time.

4.7 Network Access

1. Users that wish to access the network using their personally owned computer may do so using only authorized software and only with the approval of the user's supervisor and the Director, DITSO.
2. Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the network, the user will NOT:
    a. Use the service as part of violating the data protection Act 2012 (Act 843)
    b. Attempt to break the security of any computer network or user
    c. Attempt to send junk email or spam to anyone
    d. Attempt to send a massive amount of email to a specific person or system to flood their server

4.8 Device Authorization:

1. DITSO reserves the right to determine the level of network access for each personally owned device. The user will be granted any of the following rights: full, partial or guest access.

2. DITSO shall install a digital certificate on each personally owned device, which will authenticate the user.

4.9 Third-Party Applications

1. DITSO reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

2. As the number of approved applications continually evolves, the user must check with the DITSO for the current list of approved third-party applications and get it approved before downloading it on the device.

4.10 Remote Wiping

1. While UESD does not own the device, they do own all company data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time. Not only will company data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk.

2. Furthermore, the user must agree to a full wipe of the personally owned device if they leave or quit the University. This may result in the loss of both company and personal data on the device.

4.11 Reporting Security Concerns

The user agrees to report the following immediately:

1. If the device is lost or stolen

2. If the device has been attacked with malware, a virus or any other suspicious attack

3. Any other security concerns with regards to company data

4.12 BYOD and Acceptable Use Policy

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of the University. It is for this reason we have established our BYOD and Acceptable Use Policy as follows:

1. All employees are expected to understand and actively participate in this program. UESD encourages all employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

2. Prior to using personal devices for company purposes, each employee is expected to have read the entire BYOD and Acceptable Use Policy.

3. If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the BYOD and Acceptable Use Policy as below:

4. I have read and understood BYOD and Acceptable Use Policy, and I understand the requirements and expectations of me as an employee.

5.0 PRINT GUIDELINE

5.0 General Guideline

Staff are required to use the University shared networked printing services (i.e., those that are connected to and can be used by more than one computer workstation) for all official printing jobs. Dedicated printers are permissible only with advanced approval from the respective Director or Dean, the Register, the Pro VC or the VC in accordance with the requirements and limitations set forth in this policy. Units and Departments are responsible for all costs associated with their printing and copying jobs, including purchase and installation of printer supplies, such as paper, toner, ink and other consumables. Shared, networked printers are provided by the University to facilitate normal business operations and dedicated use by Departments and Units. DITSO shall provide support for all units and departments.

5.1 Staff and Student Printing Services

This document outlines the University's approach to utilization of printing and copying services on campus. The goal of this policy is to facilitate efficient and cost-effective use of printing and copying services and assets. This policy applies to anyone utilizing printing facilities provided by the University. The University is committed to promoting sustainable and environmentally friendly printing services, as such staff are encouraged to be diligent with the volume of printing and copying that they do. Therefore, any staff's printing and copying behavior that exceeds 500 pages per month, will be flagged and surcharged to his/her salary.

The printing and copying services provided by the University are not intended for personal use or non-work-related documents. Staff are encouraged to use the mono printing option whenever possible to reduce costs and demand on limited color print resources.

5.2 Use of Dedicated Printers

Employees whose role very frequently involves the need to print confidential documents will be permitted to use a dedicated, non-networked printer. Since shared printers have a security feature enabling users to protect the privacy of their printed documents, employees who occasionally have the need to print confidential documents will not qualify for a dedicated printer. Anyone using a shared printer to print confidential documents must use that shared printer's print and release functionality. All dedicated printers will be purchased using unit/departmental funds and will be exclusively maintained and supplied by the unit/department. DITSO shall provide support for all installed dedicated printers. All dedicated printers will be of a brand and type specified by DITSO and must be purchased according to established procurement procedures provided by the Procurement Unit.

5.3 Private Printers

Any privately owned printer will not be connected to the University's printing network. Any network printing support provided by DITSO is not available to privately owned printers. The University will not fund consumables for private printers. The owners of any privately owned printer connected to the network shall be requested to be removed and the violation reported for disciplinary action to be taken by the ICT Committee.

5.4 Acquisition of Printing Services

All requests for Printing Service can be initiated by completing forms available on the University website. All staff print services will be accessed in accordance with the following criteria:

1. Every request for new or amended printing services will be appropriately assessed by the Print Management Solution so as to ensure that the most suitable service is deployed in a timely manner.

2. DITSO shall ensure that every office has appropriate access to suitable standard print services in order to meet the printing and photocopying requirements of staff in that office.

3. The acquisition and use of individual private printer services is prohibited unless it can be deemed to be an exception, or it has been granted an exception by the Vice Chancellor.

4. When print services are no longer required in an office, DITSO shall be notified by completing the appropriate forms on the University website.

6.5 Data Center Access/Authorization Request

6.5.1. Departments/Schools/Units

Departments/schools/units that have computer equipment in the Data Center may request access to the Data Center. The individuals designated by the requesting departments/schools/units will be granted access once DITSO authorizes them. Upon approval by DITSO, an appointment with the person requesting access will be scheduled to provide the person with a copy of the UESD Data Center Access Policies. When a person who has access to the Data Center terminates his employment or transfers out of the department, the person's department must notify DITSO as soon as possible so that the person's access to the Data Center can be removed. This is extremely important in cases where the employee was terminated for just cause.

University staff members must be pre-approved for unescorted access within the Data Center. Vendor access must be sponsored by an authorized staff member, or director, or department/unit head. Authorizations will only be approved for individuals who are responsible for installation and/or maintenance of equipment housed in the Data Center. Approval processes are as follows:

1. Authorization forms must be signed by the director, or department head of the person requesting access.
2. After approval, the Head, NST will review and approve.
3. If approved, the authorized staff member or vendor will be added to the authorization database, and the authorization form will be kept on file.
4. Authorized staff/vendors will be allowed entrance into the Data Center by a Data Center employee but will then have unescorted access within the Data Center.
5. Authorized staff/vendors are responsible for logging in/out when entering/exiting the Data Center. The purpose of the visit must be documented.

6.5.2 Visitors

Anyone who is not a Data Center employee, an authorized staff member, or authorized vendor is considered a visitor. All visitors to the Data Center must adhere to the following procedures:

1. All visitors must enter through the main entrance of the Data Center.
2. Visitors must be always accompanied by either a Data Center employee or other authorized staff member while in the Data Center. Exceptions to this policy must have the approval of the Director, DITSO

1. Visitors must log in/out when entering/exiting the Data Center. The purpose of the visit must be documented.
2. Visitors must always wear a visitor's badge/tag.
3. Visits should be scheduled through the Head, NST at least 24 business hours in advance. Unscheduled visits to install equipment or perform other tasks may be turned away.

6.6 General Data Center Operations Guidelines

General Hosting Policy for Data Center Capacity Planning. DITSO must be consulted for any new equipment to be installed in the Data Center. It is advisable to consult with the directorate as early as possible (preferably months before actual equipment is ordered), to confirm the equipment can be hosted

4. General Policy on Infrastructure Work in The Data Center. DITSO must be notified of all work pertaining to infrastructure in the Data Center. This includes things such as equipment installation/removal, construction or any activity that adds/removes assets to/from the Data Center.

6.7 General Cleanliness Guidelines

The Data Center must be kept as clean as possible. All individuals in the Data Center are expected to always keep clean the vicinity. Boxes and trash need to be disposed of properly. Tools must be replaced to their rightful place. Food and drink are not allowed in the Data Center.

6.8 Data Center Equipment Deliveries/Pick-Up

Any department that is planning to have equipment delivered to or picked up from the Data Center should contact ITS Operations and provide details to ITS Operations in advance of delivery/pick-up. DITSO must be provided with the following information for equipment log.

For the delivery of equipment:

1. Expected day of delivery
2. P.O. number for the equipment (if known)
3. Vendor name and description of the equipment
4. Person to be contacted when the equipment arrives

For the pick-up of equipment:

1. Expected day the equipment will be picked up
2. Vendor name and the description and location of the equipment to be picked up.
3. Name of person to be notified once equipment is picked up

6.9 Audit Procedures

1. DITSO Data Center will send a list of authorized staff and authorized vendors to the appropriate directors, or department heads on a quarterly basis (January, April, July, and October) for review and verification.

2. Each director/department head will review and update the list of authorized staff/vendors and return it to the Head, NST within two weeks.

3. Failure to return access audits will result in revocation of access privileges for previously authorized staff/vendors until such time as the audit is returned.

    a. Equipment Installation: Authorized staff performing the installation must submit an installation form.

    b. Equipment Removal: Authorized staff performing the removal must submit a removal form.

    c. Equipment Renaming: Authori zed staff performing the rename must submit a rename form.

6.0 DATA CENTRE ACCESS GUIDELINES AND PROCEDURES

6.0 Data Center Equipment

To maximize security and minimize disruptions, the following apply to all equipment housed in the Data Center.

1. A form must be completed for all equipment installations, removals, and changes.
2. Data Center employees will deny entry to authorized staff or vendors who intend to install, remove, or rename equipment without an accurate equipment form.
3. Equipment housed within the Data Center must meet relevant industry standard system specifications.

6.2 Data Center Access

To ensure the systems housed within the data center are kept secured, the following policies apply to all personnel requiring access:

1. All personnel who access the Data Center must have proper authorization. Individuals without proper authorization will be considered as visitors.
2. Visitors to the Data Center must adhere to the visitors' guidelines below.
3. Authorizations will be verified on a quarterly basis.
4. All personnel must always wear a valid University or vendor identification badge.
5. All personnel must sign in when entering the Data Center to document the time and purpose of their visit. They also must sign out when leaving.
6. All personnel must enter through the Data Center's main entrance and must always wear a University ID or visitor's ID.
7. Authorized staff will have access to the Data Center at any time.
8. Systems housed within the Data Center that contain data classified as Level III or above will be monitored by Data Center employees through live video cameras.

6.3 Levels of Access to the Data Center

There are 3 "Levels of Access" to the Data Center in UESD:

1. General Access,
2. Escorted Access and
3. Limited access

6.3.1 General Access

General Access is given to people who have free access authority into the Data Center. General Access is granted to DITSO staff whose job responsibilities require that they have access to the area. Individuals who are granted general access may access DITSO data center and disaster recovery areas via key access. Key access is granted by property control after appropriate permission is obtained from either the Director of DITSO or the Head of Network, Systems and Telecommunication unit. Individuals with Limited access will be granted a different key combination for the data center door. Individuals with General access to the area may allow properly authorized individuals with escorted access to the data center. If a person with General Access allows Escorted access to an individual, the person granting access is responsible for escorting the individual with granted access and seeing to it that the protocol is followed.

6.3.2 Escorted Access

Escorted access is closely monitored access given to people who have a legitimate business need for infrequent access to the Data Center. "Infrequent access" is generally defined as access required for less than 15 days per year. Individuals with Escorted Access will not be issued a door key to access the data center with. A person given Escorted Access to the area must sign in and out under direct supervision

of a person with General Access, must provide positive identification upon demand, and must leave the area when requested to do so.

6.3.3 Limited Access

Limited Access is granted to a person who does not qualify for General Access but has a legitimate business reason for unsupervised access to the Data Center. Unescorted Access personnel cannot authorize others to be granted unsupervised access to the Data Center. Unescorted access personnel can only grant escorted access to individuals whose activity relates to the grantor's business in the Data Center. The grantor is responsible for these individuals and must always escort them into the Data Center.

6.4 Data Center Door

All doors to the Data Center must always remain locked and may only be temporarily opened for periods not exceeding what is minimally necessary to:

1. Allow officially approved and locked entrance and exit of authorized individuals permit to transfer supplies/equipment directly supervised by a person with General Access to the area

2. Prop the door open to the Data Center ONLY if it is necessary to increase airflow into the Data Center in the case of an air conditioning failure. In this case, personnel with General Access must be present and limit access to the Data Center.

6.5 Data Center Access/Authorization Request

6.5.1. Departments/Schools/Units

Departments/schools/units that have computer equipment in the Data Center may request access to the Data Center. The individuals designated by the requesting departments/ schools/units will be

6.5 Data Center Access/Authorization Request

6.5.1. Schools/Departments/Units

Departments/schools/units that have computer equipment in the Data Center may request access to the Data Centre. The individuals designated by the requesting departments/ schools/units will be granted access once DITSO authorizes them. Upon approval by DITSO, an appointment with the person requesting access will be scheduled to provide the person with a copy of the UESD Data Centre Access Policies. When a person who has access to the Data Center terminates his employment or transfers out of the department, the person's department must notify DITSO as soon as possible so that the person's access to the Data Center can be removed. This is extremely important in cases where the employee was terminated for just cause.

University staff members must be pre-approved for unescorted access within the Data Center. Vendor access must be sponsored by an authorized staff member, or director, or department/unit head. Authorizations will only be approved for individuals who are responsible for installation and/or maintenance of equipment housed in the Data Centre. Approval processes are as follows:

1. Authorization forms must be signed by the director, or department head of the person requesting access.

2. After approval, the Head, NST will review and approve.

3. If approved, the authorized staff member or vendor will be added to the authorization database, and the authorization form will be kept on file.

4. Authorized staff/vendors will be allowed entrance into the Data Center by a Data Center employee but will then have unescorted access within the Data Center.

5. Authorized staff/vendors are responsible for logging in/out when entering/exiting the Data Center. The purpose of the visit must be documented.

6.5.2 Visitors

Anyone who is not a Data Center employee, an authorized staff member, or authorized vendor is considered a visitor. All visitors to the Data Center must adhere to the following procedures:

1. All visitors must enter through the main entrance of the Data Center.
2. Visitors must be always accompanied by either a Data Center employee or other authorized staff member while in the Data Center. Exceptions to this policy must have the approval of the Director,

DITSO

1. Visitors must log in/out when entering/exiting the Data Center. The purpose of the visit must be documented.
2. Visitors must always wear a visitor's badge/tag.
3. Visits should be scheduled through the Head, NST at least 24 business hours in advance. Unscheduled visits to install equipment or perform other tasks may be turned away.

6.6 General Data Center Operations Guidelines

1. General Hosting Guideline for Data Center Capacity Planning. DITSO must be consulted for any new equipment to be installed in the Data Center. It is advisable to consult with the directorate as early as possible (preferably months before actual equipment is ordered), to confirm the equipment can be hosted
2. General Guideline on Infrastructure Work in The Data Center. DITSO must be notified of all work pertaining to infrastructure in the Data Center. This includes things such as equipment installation/ removal, construction or any activity that adds/removes assets to/ from the Data Centre.

6.7 General Cleanliness Guideline

The Data Centre must be kept as clean as possible. All individuals in the Data Centre are expected to always keep clean the vicinity. Boxes and trash need to be disposed of properly. Tools must be replaced to their rightful place. Food and drink are not allowed in the Data Centre.

6.8 Data Centre Equipment Deliveries/Pick-Up

Any department that is planning to have equipment delivered to or picked up from the Data Centre should contact ITS Operations and provide details to ITS Operations in advance of delivery/pick-up.

DITSO must be provided with the following information for equipment log.

For the delivery of equipment:

1. Expected day of delivery
2. P.O. number for the equipment (if known)

3. Vendor name and description of the equipment

4. Person to be contacted when the equipment arrives

For the pick-up of equipment:

1. Expected day the equipment will be picked up

2. Vendor name and the description and location of the equipment to be picked up.

3. Name of person to be notified once equipment is picked up

6.9 Audit Procedures

1. DITSO Data Center will send a list of authorized staff and authorized vendors to the appropriate directors, or department heads on a quarterly basis (January, April, July, and October) for review and verification.

2. Each director/department head will review and update the list of authorized staff/ vendors and return it to the Head, NST within two weeks.

3. Failure to return access audits will result in revocation of access privileges for previously authorized staff/ vendors until such time as the audit is returned.

a. Equipment Installation: Authorized staff performing the installation must submit an installation form.

b. Equipment Removal: Authorized staff performing the removal must submit a removal form.

c. Equipment Renaming: Authorized staff performing the rename must submit a rename form.

7.0 DISASTER RECOVERY AND BUSINESS CONTINUITY

Table 7.1. Definition of terms

Disaster	A disaster refers to an event which leads to an extended loss of service or loss of critical data and cannot be managed within the scope of normal working operations.
Mission-Critical Data	The following forms of information are deemed operationally critical by the UESD management and are therefore subject to this Policy: [Note: This section attempts to classify the applications, databases, and data structures in use in your facility. Identify them here. Technical Manager to specify more details] **These items can be graded as Low, Medium, High**

Critical IT Systems	Grade
Network	High
LMS and E-learning platforms (cloud solutions)	High

7.1 Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help UESD recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.

Additional objectives include the following:

1. The need to ensure that all employees fully understand their duties in implementing such a plan
2. The need to ensure that operational policies are adhered to within all planned activities
3. The need to ensure that proposed contingency arrangements are cost-effective
4. The need to consider implications on other campus sites
5. Disaster recovery capabilities as applicable to key stakeholdersIt is the responsibility of an IT Auditor (Executive Authority) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of the DIRECTOR, DITSO (Technical Authority) to verify the practices and procedures necessary to execute this policy.

7.2 General Guidelines

DITSO shall ensure that:

1. A comprehensive IT disaster recovery plan is developed.
2. A formal risk assessment is undertaken to determine the requirements for the disaster recovery plan
3. The disaster recovery plan covers all essential and critical infrastructure elements, systems and networks
4. The disaster recovery plan is periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
5. All staff are made aware of the disaster recovery plan and their own respective roles.
6. The disaster recovery plan is kept up to date to take into account changing circumstances.

7.3 Disaster Declaration

The Director, DITSO is authorized to declare an Information Technology Systems Disaster to the University community and also signal a resumption of normal operations:

7.4 Plan Activation

1. Disaster Recovery plan will be activated in response to internal or external threats to the Information Technology Systems of UESD. Internal threats could include fire, bomb threat, and loss of power or other utility or other incidents that threaten the staff and/or the facility.
2. External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community.
3. Once a threat has been confirmed, the disaster recovery plan management team will

assess the situation and initiate the plan if necessary.

7.5 Resumption of Normal Operations

Once the threat has passed, equipment has been repaired or replaced or a new data center has been built and stocked, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations. **7.6 Disaster Recovery Strategy**

The overall disaster recovery strategy of UESD is as below;

7.6.1 Data Center Disruption

1. Failover to alternate Data Center
2. Reroute core processes to another Data Center (without full failover)
3. Operate at a deprecated service level
4. Take no action

7.6.2 Significant Dependency (Internal or External) Disruption

1. Reroute core functions to backup or alternate provider
2. Participate in recovery strategies as available
3. Wait for the restoration of service, provide communication as needed to stakeholders

7.6.3 Significant network Disruption or other related issues

1. Reroute operations to backup processing unit / service (load balancing, caching)
2. Wait for service to be restored, communicate with core stakeholders as needed

7.7 Disaster Recovery Plan

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.

1. Response Phase: The immediate actions following a significant event.
    a. On call personnel will be engaged
    b. Decision made around recovery strategies to be taken
    c. Full recovery team identified
2. Resumption Phase: Activities necessary to resume services after team has been notified.

a. Recovery procedures implemented

b. Coordination with other departments executed as needed

3. Restoration Phase: Tasks taken to restore service to previous levels.

c. Rollback procedures implemented

d. Operations restored

7.8 Disaster Recovery Operations

1. All activities and steps necessary to restore systems services that are affected by a disaster.
2. All activities concerned with management and user communications related to the disaster.
3. All activities concerned with the mitigation of the impact of an ongoing disaster incident.
4. All activities concerned with the follow-up to an incident.

7.9 Disaster Recovery Standards

1. Each department shall have a documented disaster recovery plan.
2. Each department's disaster recovery plan shall include a clear definition for disaster, specific to their facilities and technology configuration.
3. Each department's disaster recovery plan shall be accessible in the event of a disaster.
4. Each department's appropriate staff shall be trained on the disaster recovery plan.
5. Each department's disaster recovery plan shall include responsibilities, authorities, and accountabilities during contingency operations.
6. Each department shall have vendor maintenance contracts to address equipment and/or system failures.
7. Each department's disaster recovery plan shall address the need for an alternative recovery site.

8.0 VIDEO SURVEILLANCE GUIDELINE

8.1 General Guidelines

The system comprises fixed position cameras, Pan Tilt and Zoom cameras, Monitors, digital recorders etc. Cameras are located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of general office workspace. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

8.2 Purpose of the Surveillance System

The system has been installed by the University with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

1. Deter people with criminal intent
2. Assist in the prevention and detection of crime
3. Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
4. Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

8.3 Security Control Room

Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry. Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room. Before allowing

access to the Control Room, staff in charge of the control room shall satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the Centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

8.4 Footage Monitoring

Video monitoring for security purposes will be conducted in a professional, ethical and legal manner and will not violate anyone's reasonable expectation of privacy. Cameras will not be installed in areas where there is a reasonable expectation of privacy. Personnel involved in video monitoring will be appropriately trained and regularly supervised in the responsible use of this technology.

Video monitoring of public areas for security purposes at UESD is limited to uses that are intended to be consistent with reasonable expectations of privacy. An individual's or a group's behavior may warrant specific monitoring with community safety in mind. However, no one will be selected for monitoring based on discriminatory criteria such as gender, race, sexual orientation, national origin or disability.

Covert video surveillance equipment may be used so long as such use is consistent with this policy and applicable law. Covert cameras will only be used to aid in criminal investigations and require approval of the District Police Commander.

Video surveillance equipment found to be illegal, installed without approval, or used in such a manner that violates any portion of this policy can and/or will be removed and/or confiscated under authority of the District Police Commander and at a cost to be billed to the violating department or individuals.

8.5 Storing and Viewing Images

When conducting a viewing, either of live images or recorded playback, the viewing should take place in a secure office and only those persons who are authorized and/or who appear on the footage, should be present where relevant. Staff should ensure that no part of the footage can be seen through a window in a door or a window

looking into the office from an external area. The office door should be completely closed for the duration of the viewing and for any discussions about the footage that may follow. In general, CCTV footage should be kept for a maximum of 30 days, unless an incident has occurred on UESD premises and the footage is to be kept for a purpose. CCTV footage is stored securely in a lockable office / on the university's password protected software system. If an incident has occurred, the footage in question should be stored securely in a way that maintains the integrity of the images pending further action. Once the action/investigation has been concluded, a review of the retention of the footage should be exercised and secured, permanent disposal of the footage should occur where there is no longer a valid lawful basis to keep the images.

The University has developed a form called the "CCTV Disclosure Record" and it must be completed on every occasion that footage is viewed or disclosed to a third party. The form should be forwarded to the Cyber Security Officer (to be replaced with right designation in DITSO orgchat) as and when a valid request for CCTV footage is made. The form can be

located on the University's internal shared drive. The record will include the following:

5. The purpose of any searches and whether the search was successful or not
6. Who carried out the search
7. Persons present (particularly when reviewing).
8. Date, start and end time of the incident.
9. Date and time of the review
10. Any other relevant information

8.6 Disclosure of images and recordings

The University shall ensure that any disclosure of images is in a controlled manner and that the disclosure is consistent with their data mapping and privacy notice in regards to CCTV. Any disclosure should be clearly documented by the University as outlined above.

There will be no disclosure of recorded data to third parties without a lawful basis. It is acceptable for the University to disclose images to law enforcement agencies for the purpose of prevention and detection of crime. These requests should be:

1. Provided in writing (WA170) where possible
2. Signed by authorized officers
3. Referenced to the name and section of the legislation that entitles them to receive the information

DITSO shall document in their records how personal information will be shared. In the case of a disclosure request from law enforcement or a valid subject access request, the recording pertaining to the request will be downloaded onto a portable device and securely stored in a locked room until collection. The process will remain the same when disclosing in regard to insurance purposes. The file will be encrypted or password protected where possible. Alternatively, the recording will be sent in a password protected document via email. Staff will ensure passwords are given to the authorized recipient separately from the email containing the recording, ensuring that the original copy of the recording is kept at the directorate for only as long as is necessary for the purpose of retaining the recording. If the immediate viewing of a recording is necessary, this will be governed by the viewing procedure mentioned above.

The data may be used within the University's discipline and complaints procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9.0 SOFTWARE INSTALLATION & LICENSING GUIDELINE

Table 9.1. Definitions and Abbreviations

Workstation	An end-user computing device such as a PC, laptop, tablet or smartphone used to access resources over the University's network.
System	A collection of elements organized for a defined purpose or objective. Systems consist of hardware, software, information, and human assets
Service	A defined set of functionality and information provided by one or more systems
Hardware	Computing and telecommunications devices including PCs, servers, routers, switches, disk units, modems etc
Information Asset	An Information Asset is defined as a computer system, service, facility, application, software, data, database, proprietary knowledge, experience, insight, etc., which has value to the University. The term encompasses all information content that requires protection against security risks. Information Assets governed by this Policy may legally belong to the University, or a third party but placed in the University's care or custodianship (such as personal data).
Information Security	General term for the risk management activity involving the implementation, operation and maintenance of controls designed to meet business requirements for confidentiality, integrity and availability of information assets by preventing incidents and/or minimizing impacts.
ISMS	Information Security Management System – the overall framework security comprising governance, policies, standards, procedures, guidelines, and other processes through which information security is directed and controlled
ITC	Information Technology Committee – the University IT governance body responsible for information security.

9.1 Software Licensing Compliance

1. Individual users of software applications have a responsibility to ensure that:

    a. Software installed on workstations for which they have some responsibility is licensed.

    b. The software is either named on the list of University list of approved and supported software, or ortherwise use of the software has been agreed with/ notified to the Director, DITSO.

    c. The software is not named on the list of prohibited software maintained at the University

    d. They are complying with the conditions of use of that license.

2. A central list of supported software approved for use within the University will be maintained by DITSO, as well as a list of specifically prohibited software (e.g. on security grounds or inappropriate use of University resources). Use of software that may not require a license, e.g. Freeware or Shareware, may only be used if it is on the list of officially approved software. Usage of approved screensavers will be specified by DITSO.

3. Each user must take responsibility (in conjunction with the authorizer and installer) for their particular use of software, under the license terms and End User License Agreement.

4. The University's Conditions of Use of Computing and Network Facilities contains the following stipulations concerning the use of licensed software – failure to comply with these could constitute a disciplinary offence:

    a. The University reserves the right for access to be granted to computer audit staff without notice to enable them to check against an inventory of licensed software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by such audit staff and reported to the Director DITSO, who may initiate disciplinary proceedings.

    b. Where software has been electronically downloaded from IT Services computer systems requiring user authentication employing a username and password, the user must read and comply with the licensing conditions for that software, and the act of downloading indicates acceptance of the licensing conditions pertinent to that software.

    c. All persons who are licensed to use software or who control access to any computing and/or network resources are obliged to take all reasonable care to prevent the illicit copying and use of software and documentation.

    d. No one shall introduce to computer systems any software or other material requiring a license for which a valid license is not in place.

9.2 Software Inventories

1. A software inventory must be set up and centrally maintained at DITSO with responsibility of the Director, DITSO.

2. This software inventory will be used to match the number of software licenses purchased against the number of staff licenses in use; also to check that the software licenses are current, i.e. have not expired. This monitoring must be carried out regularly, and licenses purchased appropriately if required to rectify any discrepancies identified.

3. The inventory must take account of staff leavers, i.e., identifying software licenses that are no longer being used. Unused software licenses remain the responsibility of DITSO. Any transfer of such licenses between schools, directorates and department should be recorded within the inventory.

4. The same managers responsible for the software inventory are also responsible for maintaining copies of the software licenses relating to the inventory.

5. Use of Freeware/Shareware software should also be monitored to ascertain firstly that use of the software is free for use for business use within the University, and secondly that the use of such Freeware/Shareware does not pose any security risks. Beyond carrying out these checks, it is not necessary to either record the usage of such software or maintains copies of software licenses.

9.3 Software Purchasing

1. Software purchasing must be limited just to DITSO, together with any other nominated individuals authorized by the requesting department/unit. A list of such additional authorized individuals must be documented and maintained by DITSO. These authorized members of staff must also sign off individual software purchases.

9.4 Storage of Software Media and Licenses

1. Software and media must be stored in a suitably secured and accessible location, and take into account the Business Continuity requirements, including for the case of loss of a server, or even potential loss of a building.

2. The location of the software media should be recorded on the software inventory.

3. Similar consideration must be given to software that has been downloaded, and it should be stored on an appropriate server. A hard copy of the license or certificate should also be stored.

9.5 Authorized installation of software

1. Only authorized IT Staff within DITSO are permitted to undertake installation of software. Other non-IT staff will be permitted to undertake installation of software only if authorized on the exception list maintained by DITSO.

2. The same IT installation staff (or other staff specifically authorized to install software) are also responsible for ensuring that the software which they are installing is appropriately licensed and recorded in the relevant software inventory.

9.6 Software Audit and Use of Audit Tools

1. Wherever possible, access to the use of the software by individuals should be controlled by Active Directory, thereby enabling both potentially automatic distribution of software applications, as well as automated use of audit tools

2. Support staff, either in IT services centrally, the university, have the responsibility for using these automated audit tools to ensure compliance by the University, i.e. confirmation that the number of licenses held corresponds with the actual number of users of the software as specified by the license conditions.

3. An exception list of those devices which are excluded from such an audit must be specified university e.g. laptops and devices on the wireless network.

4. All University workstations and servers must have the standard corporate tools installed on them as part of their build to enable the software monitoring to take place. Any exception to this must be authorized and documented at DITSO.

5. If suitable automated tracking software is available, support staff should use this to identify any software which may no longer be required within the University, with a view to either re-utilizing such software or arranging for its disposal if redundant.

9.7 Disposal of Software

When permanently disposing of equipment containing storage media, all licensed software must be irretrievably deleted either before the equipment is moved off-site, or by utilizing an approved 3rd party off-site service.

9.8 Staff Responsibilities

- Heads of Unit

Responsibilities of DITSO Heads of Units in respect of software licensing staff can be summarized as follows:

a. Maintaining a University list of approved/supported software.

b. Maintaining a University list of prohibited software.

c. Maintaining a software inventory for the University.

d. Maintaining copies of the software licenses relating to the inventory.

e. Ensuring that IT support staff carry out a regular automated audit of software in use on workstations.

6. IT Services Staff Authorised to Install Software

Responsibilities of IT Services staff authorised to install the software in respect of software

licensing can be summarised as follows:

a. Ensuring, with the user, that software being used on the workstation is licensed, and approved/not prohibited.

b. Ensuring with the users that they are complying with the conditions of the software licence.

c. Ensuring that the installed software is recorded in the software inventory.

7. University Staff Using Workstations

Responsibilities of University staff using workstations in respect of software Licensing can be summarised as follows:

a. Ensuring that software being used on the workstation is licensed, and approved/ not prohibited.

b. Ensuring that they are complying with the conditions of the software license.

10.0 EMAIL ACCOUNT USE GUIDELINE

10.1 Administrative Use

This guideline describes the Email procedure to be used by the University of Environment and Sustainable Development (UESD) as a means of communication both internally and externally. In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic and other official purposes. E-mail for formal communications facilitates the delivery of messages and documents to campus and communities outside campus or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. It is a policy of UESD that all staff and students observe the electronic mail policy to ensure proper use of the University's electronic communication system.

10.2 Purpose

The UESD email service supports the educational and administrative activities of the University and serve as an enhanced means of official communication by and between users of UESD. The purpose of this policy is to ensure that these critical services remain available and reliable, and are used for purposes appropriate to the University's mission. Also, to make users aware of what UESD deems as acceptable and unacceptable use of its email system.

10.3 Scope

This guideline covers the use of all email addresses issued by DITSO to all staff and students. These communications may include administrative content, such as Human Resource (HR) information, policy messages, general University messages, official announcements, etc.

10.4 Responsibility and Authority

It is the responsibility of the departmental heads (executive authority) to execute and monitor the effectiveness of this policy, and to administer corrective action when it is deemed necessary or warranted. It is the responsibility of the Systems Administrator to verify the practices and procedures necessary to execute this policy.

10.5 General Guideline

1. Email Addresses and Accounts Creation – Faculty, Staff and Students

When an employee joins the institution, the Human Resource Department (HRD) initiates the request and ask DITSO to create official Email for the new employee as well as to delete same when this employee leaves UESD (Exit Clearance). DITSO then notifies HR by email once the new account is created. For access to the University's email account details (Username and Default Password), the newly created user must contact DITSO. Once a user's services are terminated, she/he may no longer access the contents of the mailboxes. Faculty and staff email users are advised that electronic data and communications using the University network for transmission or storage may be reviewed and/or accessed by authorized University officials for purposes relating to University business. DITSO has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.Email services are available for students to support learning and for communication by and between the University and themselves. The services are provided only while a student is enrolled in the University and once a student leaves the enrolment of the University, the student would no longer access the contents of the mailbox. Student email users are advised that electronic data and communications using the University network for transmission or storage may be reviewed and/or accessed in accordance with the UESD Acceptable Use Policy. DITSO has the authority to access and inspect the contents of any equipment, files or email on its electronic systems. DITSO has separate domain names for staff and students. The UESD standard E-mail Account Format for staff is as follows:

Full Name: Joseph Kofi Armah Boah

Email: jkaboah@uesd.edu.gh

The UESD standard E-mail Account Format for students are: jm.uesd.edu.gh and gs.uesd. edu.gh for junior members and graduate students respectively.

Hence undergraduate and graduate students would have emails as follows:

a. jkaboah@jm.uesd.edu.gh for junior members

b. jkaboah@gs.uesd.edu.gh for graduate students

With this format, the initials of all names preceding the Surname/Last name are used.

1. In cases where email addresses conflict, uniqueness is ensured by adding numbers to the end of the

surnames of subsequent emails. For example:

Full Name: John Kuuku Asiedu Boah

To create this as the subsequent email address, it will be:

a. jkaboah1@uesd.edu.gh for staff

b. jkaboah1@jm.uesd.edu.gh for junior members

c. jkaboah1@gs.uesd.edu.gh for gradute student

10.6 Email Account Deletion

Accounts will be disabled on the termination date specified by HR by initiating a request to the DITSO. When it is anticipated that University business-related email may continue to be sent, the HRD may request a temporary auto-reply on a former employee's email account to instruct senders where to direct such business for a period to be determined by the University Management.

10.7 Acceptable Use

Email users have a responsibility to learn about and comply with UESD policies on acceptable use of UESD electronic services. Violation of these policies may result in disciplinary action dependent upon the nature of the violation. Examples of prohibited uses of email include:

Intentional and unauthorized access to other people's email;

Sending "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail;

Use of email for commercial activities or personal gain (except as specifically authorized by university policy and in accordance with university procedures);

1. Use of email for partisan political or lobbying activities;
2. Sending of messages that constitute violations of UESD's Code of Conduct;
3. Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications;
4. Use of email to transmit materials in a manner which violates copyright laws;
5. Using the facility for illegal/commercial purposes is a direct violation of this policy and may result in withdrawal of the facility;
6. Unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages;
7. Generation of threatening, harassing, abusive, obscene or fraudulent messages/images;
8. In sending large attachments to others, user should make sure that the recipient has email facility that allows him/her to receive such large attachments;
9. Opening any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and it contains any attachment that is of suspicious nature or looks dubious, the recipient should get confirmation from the sender about its authenticity before opening it;
10. Impersonating email account of others will be taken as a serious offence under the University's IT security policy;
11. Keeping the mail box used space above 80% usage threshold. The indication of a 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments. This is very much essential from the

point of security of the user's computer, as such messages may contain viruses that have the potential to damage valuable information on the user's computer;

12. User sharing his/her email account with others is prohibited, as the individual account holder is personally accountable, in case of any misuse of that email account;

13. Intercepting, or trying to break into others email accounts is an infringement on the privacy of other users;

14. When using computers that are shared by other users, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

10.8 E-Mail Auto-Forward

This guideline prohibits the use of the External Auto-Forward feature where every e-mail sent to an UESD e-mail account is automatically forwarded to a third-party non-UESD account. External Auto-Forward can be problematic because it can lead to inadvertent transmission of sensitive or restricted information to external networks. Auto-Forward is also problematic because UESD cannot ensure nor verify that the forwarded message was received by an external e-mail system.

11.0 PASSWORD GUIDELINE

11.1 General Guideline

Passwords are used for various purposes at UESD. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong/ compliance passwords.

11.2 Password Creation

All Users shall create a strong password for any UESD resources granted to them and must conform to the password creation guidelines described below.

All Users must not use the same password for UESD accounts as for other non-UESD access (for example, personal yahoo.com or Gmail account, Facebook account, trading site, dating site, and etc). All user-level and system-level passwords must conform to the guidelines described below.

User accounts that have system-level privileges granted through group memberships must have a different password from all other accounts held by that user.

Where possible, users must not use the same password for various UESD access needs.

11.3 Password Creation Guidelines

Every User should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

1. The password contains less than eight (8) characters and the password is a word found in a (English or foreign) dictionary.
2. The password is a common usage words such as names of family, pets, friends, co-workers, fantasy characters, etc.
3. Computer terms and names, commands, sites, companies, hardware, software.
4. Birthdays and other personal information such as addresses and phone numbers.
5. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
6. Any of the above spelled backward.

7. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

1. Contain both upper- and lower-case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|- =\`{}[]:";'<>?,./)
3. Are at least eight alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.

Are not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, the phrase might be: "One way I can remember my password" and the password could be: "Ow1crMp#" or "1Wic?mp/" or some other variation.

11.4 Password Protection Standards

Do not share UESD passwords with anyone, including system Administrators or your head of unit/department.

All passwords are to be treated as sensitive and confidential UESD information.

If someone demands a password, refer him or her to this document or have him or her call someone in the DITSO team for assistance.

If an account or password is suspected to have been compromised, report the incident to DITSO and change all passwords.

Here is a list of **"DON'TS":**

5. Never write down a password or store it online
6. Don't reveal a password over the phone to ANYONE
7. Don't share username and password in the same email message, SMS and any other social media.
8. Don't reveal a password to your supervisor
9. Don't talk about a password in front of others
10. Don't hint at the format of a password (e.g., "my family name")
11. Don't reveal a password on questionnaires or security forms
12. Don't share a password with family members
13. Don't reveal a password to co-workers while on vacation
14. Don't use the "Remember Password" feature of applications (e.g., Internet Explorer, Google Chrome, Firefox, Instant Messenger etc)
15. Do not write passwords down and store them anywhere in your office.

16. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

11.5 Forgotten Passwords

Users will occasionally forget their password.

A characteristic of password files is that passwords cannot be looked up.

If a user forgets their password, the password can be changed by DITSO staff by opening a service request.

11.6 Password Change

All user-level passwords (e.g., Domain User Account, User Account on Network devices and Storage device etc.) must be changed every six (6) months.

All system-level passwords (for example, root, enable/secret, Domain Admin, Application Administration accounts, EMC Admin, SysAid, and so on) must be changed every three (3) months.

All vendor default password information (e.g cisco/cisco, admin/admin etc) should be changed immediately after the installation of the systems/ or software or network devices.

11.7 Password and Account Requirements for all users

All computer user accounts SHALL be secured, and they SHALL be secured by a password in accordance with this policy. For the avoidance of doubt: if a password is being used to secure an account it SHALL be created and maintained in accordance with this policy.

Systems that do not use University user details and that are primarily or exclusively intended for use by users who are not staff or students of the University SHALL be exempt from this policy, though it is recommended that such systems use this policy as a source of best practice advice, and SHOULD use “regular expression” parsing to prevent users using UESD user-details.

Other than super-user accounts, all user-details assigned to an account SHALL be subject to the same policy, and the passwords associated with those accounts SHALL be synchronised. Super-user accounts SHALL NOT be synchronized to the account/s user and SHALL NOT be managed through the Identity Management

Passwords MUST only be set by the user. Where a temporary password has been set by the Directorate or pre-set by some other means, then the user SHALL be required to change their password on first use.

A password SHALL conform to the minimum and maximum lengths as specified by DITSO. An acceptable password for an account MUST NOT be a password that is one of the five most recently used passwords for that account, and ideally systems SHOULD never allow a password to be reused.

Where a password for an account has been entered incorrectly at least three consecutive times then the account SHALL be “locked out” for one hour.

12.0 WEB CONTENT MANAGEMENT GUIDELINE

12.1 Website Hosting Guideline

The University's website is an important tool for achieving the University's mission. Its multiple uses are bound by legal, professional and ethical requirements. This policy identifies the principles that must guide website publishing and hosting at the University of Environment and Sustainable Development. The policy is applicable to anyone intending to publish on or in any University owned or controlled web resource.

12.1.1 Scope

1. This policy provides the principles that will govern:
    a. Web-based content
    b. The processes surrounding the publishing and hosting of web-based content on the University website

This policy specifically covers content management, disclaimer, web hosting, web publishing sponsorship and advertising, accessibility and legislation.

12.1.2 General Guidelines

2. The University considers web publishing to be a key strategic resource for communication, teaching, research, marketing, and administration. Appropriate use of this technology by the University community is required.
3. University resources may only be used to create and publish web pages where the purpose and effect of the published information is in support of the University's objectives and Strategic Plan. This means that the content of web pages hosted on university resources must relate to the activities and functions of the University or relate to the specific role of members of the University community.
4. Personal home pages are permissible under this policy to the extent that they contain information about the official functions and responsibilities of the University staff member.
5. Web-based publishing has an important impact on the reputation and standing of the University and must therefore occur in the context of an official policy framework. The following principles and requirements apply to all information published on the University's website.

12.1.3 Content Management

1. The University of Environment and Sustainable Development website must be based on content that has been subjected to review and authorization before publishing, to ensure that all information is accurate, up to date, relevant, consistent, and compliant with the University's policies and guidelines.
2. All information published on the University web servers must be authorized by the Head of the Website Editorial Committee.
3. There will be one Content Area Member for each Content Area of the Website. A Content Area Member will be a senior member identified by management committee.
4. Where Content Areas are "shared" or "referenced" by other Content Areas content will be referenced and not replicated.
5. There will be a nominated content owner for all content on the website. A content owner shall be a senior staff identified by the head of department/unit.
6. The Webmaster shall be responsible for the implementation of the approved/ recommended content from the Website Editorial committee. The Head of the Website Editorial committee shall submit content to the Webmaster for publication.

12.1.4 Web Hosting

1. All University-owned websites including controlled entities must be hosted on www.uesd.edu.gh
2. No University websites can be hosted outside of this domain.
3. The University may permit the hosting of web pages for external organizations where there is a clear relationship with the organization (e.g. a research partnership). Approval will be the responsibility of the Director of DITSO.
4. Where the websites of external organizations are hosted on the University website, their objects and information must comply with this policy and must align with the strategic goals of the University.

12.1.5 Sponsorship and Advertising

1. Advertising for the purposes of commercial gain is not permitted. A site cannot, for example, run advertisements as a revenue-raising venture.
2. Advertising on the University's websites of private or personal consultancy services or businesses of any kind by university staff or students, is not permitted.
3. Web pages must not include software (such as page hit counters) that carries 'built-in' advertising.
4. Mention of a sponsor's contribution is permissible, where the sponsorship is for an activity relevant to the mission and goals of the University and relevant to the content of the web page. The sponsor must give consent.

5. The inclusion of links to the website of companies sponsoring official University conferences or projects is permitted.

6. Notwithstanding the above, mention of sponsors' names is not allowed on the main entry-points to the website (e.g. University home page, School home pages).

7. All web pages containing promotional-style references to external organizations or individuals should be referred to the Director of DITSO for approval

8. Mention of the particular software that was used to create a web page is not appropriate; nor are links to the personal or business pages of the web authors.

12.1.6 Disclaimers

- Any wording of disclaimers used on the web will be provided and/or approved by the Legal Unit following consultation with relevant staff.

12.2 Social Media Guidelines

This is intended to assist UESD staff make appropriate use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, which include but are not limited to Twitter, Facebook, LinkedIn, YouTube and Instagram. It outlines the standards we require UESD staff to observe when using social media, the circumstances in which we will monitor the use of social media and the action to be taken in respect of breaches of this policy. This policy supplements the Internet and Email Guideline.

12.2.1 Social Media Guidelines

1. Using social media sites in the name of UESD:

    a. Only the Webmaster is permitted to post material on a social media website in the name of UESD and on behalf of UESD. Any repetitive breach of this restriction will amount to gross misconduct and shall be referred to the Disciplinary committee of the University.

2. Requirements / Expectations

    a. All communications made using social media which promote university services can only be made by Communications Officer and must have been through the formal approval process.

3. Using work-related social media

4. We recognize the importance of the internet in shaping public thinking about our university and our services, employees, partners and students. We also recognize the importance of our staff joining in and helping shape UESD conversation and direction through interaction in social media.

    a. You are therefore permitted to interact on [approved] social media websites about industry developments and regulatory issues. Approved social media

websites are:

» Facebook

» Twitter

» Instagram

» LinkedIn

» Whatsapp

This list may be updated by the Directorate of DITSO.

1. Personal use of social media sites

    a. The directorate permit the incidental use of social media websites for personal use subject to certain conditions set out below. However, this is a privilege and not a right. It must neither be abused nor overused and we reserve the right to withdraw our permission at any time at our entire discretion.

    b. The following conditions must be met for personal use to continue:

o use must not interfere with business or office commitments;

    i. use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);use must not interfere with business or officecommitments;

    ii. Use must comply with our policies including the Internet and Email Policy.

2. Rules for use of social media

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

1. Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
2. Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Human Resources Manager.
3. Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.
4. It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticizing it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.
5. Before you include a link to a third-party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it

is clear to the user that they have moved to the third party's website.

6. When making use of any social media platform, you must read and comply with its terms of use.
7. Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.
8. If you notice any content posted on social media about UESD (whether complementary or critical) please report it to the Director DITSO

13.0 DATABASE USE GUIDELINE

13.1 Definitions

Data Access - Flow of information between a data store and a user, system, or process. A user, system, or process is considered to have access to data if it has one or more of the following privileges: the ability to read or view the data, update the existing data, create new data, delete data or the ability to make a copy of the data. Access can be provided either continually or on a one-time or ad hoc basis. Transferring any data from one party to another in any medium can be equated to permitting access to those data.

Institutional Data - Those data, regardless of format, that is maintained by the University for reference or use by multiple University departments/units. Institutional Data does not include data that is the personal property of a member of the University community, research data, or data created and/or kept by individual employees or affiliates for their use. Examples of Institutional Data include student education records, payroll records, human resources records, and enterprise directory records.

Sensitive Institutional Data - Those Institutional Data that contain information that can be classified as either "sensitive" or "restricted". Some examples of Sensitive Institutional Data include Institutional Data that are personally identifiable and contain Social Security Numbers, bank account information, health information, or student education records.

Data User - An individual that has been authorized to access data for the performance of his/her job duties

13.2 Database Ownership

The University of Environment and Sustainable Development is the sole owner of the institutional data and through authorized personnel shall provide and approve access to Institutional Data to ensure that access to sensitive data is authorized; sensitive data with a need for protection are used appropriately and that authorized access complies with the UESD Privacy Policy and relevant acts.

13.3 Custodians of Data

A Custodian of Data is a university employee or a party acting on the behalf of the University who has been granted responsibility for managing designated data and/or data resources in his or her functional area with the help from the DITSO through the Database Administrator. A data custodian is responsible for data acquisition, maintenance, interpretation and definition, application of business rules, integrity and security, and application of access rules. Additionally, a Data Custodian must comply with any government regulations covering the data they manage. The Data custodian retains the right to approve and grant access to Sensitive Institutional Data. Access shall be granted only to those employees, affiliates, and systems that need access to perform their jobs or duties. In giving authorization for use of data the "Least

Privilege" principle must be enforced this means granting the minimum system resources and authorizations needed to perform a function or restricting access privileges of Authorized Individuals to the minimum functions necessary to perform their job. Users granted access to university data must use it responsibly only using the data for its intended purpose and respecting the privacy of members of the university community. Data Users must maintain the confidentiality of the data in accordance with all the existing policies. Authorized access to Sensitive Institutional Data does not imply authorization for copying, further dissemination of data, or any use other than the use for which the employee was authorized.

13.4 Database Administrators

Database administrators are individuals concerned with the Technical know-how of making sure one can easily use the institutional data and to find the information they need and that the system performs as it should. They sometimes work with management to understand the data needs.

Database administrators often plan security measures, making sure that data is secured from unauthorized access. Many databases contain personal or financial information, making security important. Database administrators are responsible for making sure sensitive employee data are not exposed to users of the University data. They also ensure the integrity of the database, guaranteeing that the data stored in it comes from reliable sources

Some of their core responsibilities are as follows:

1. Identifying user needs to create and administer databases
2. Ensuring that the database operates efficiently and without error
3. Making and testing modifications to the database structure when needed
4. Maintaining the database and updating permissions
5. Merging old databases into new ones
6. Backing up and restoring data to prevent data loss

13.5 MIS Component

MIS has four components namely Executive, Hardware, Software and Organizational Procedures.

Executive: These are people who utilize MIS for data needs to achieve organizational goals like planning and decision-making.

Hardware: The hardware components of MIS include various input and output devices that help in feeding data as well as displaying the information when required.

Software: Computer programs that are designed to do a specific task, for example, MS Office for Document processing etc.

Organizational Procedures: These are sets of rules or guidelines that that has been established for the use of a computer-based information system. Procedures are usually different for each organization or even across different departments/units of the same organization.

14.0 CLOUD COMPUTING SERVICES GUIDELINE

14.1 Definitions

Cloud computing is a computing model that allows for easy, on-demand computing resources (networks, servers, storage, applications and services) that can be quickly provisioned and de-provisioned with minimal interaction and is accessible to users via the internet. Cloud computing can be defined as the utilization of servers or information technology hosting of any type that is not controlled by the university. These providers expose their computing resources as a set of services. Infrastructure as Services (IaaS); Platform as a Service (PaaS); Software as a Service (SAAS)

Infrastructure as a Service: IaaS provides enterprises with storage, server, and networking options that don't require them to purchase and maintain vast private server rooms that take up a lot of energy and space.

Platform as a Service: This is similar to IaaS but in this case, most of the maintenance and configurations needed for services to run are done by the cloud provider.

Software as a Service: This refers to software products that run on the cloud providers' infrastructure they are usually multi-tenant applications that are subscribed to by the organization. Examples include: Dropbox, Google Drive/Docs, third party email providers such as Gmail.

Service Level Agreement: A service-level agreement (SLA) is a commitment between a service provider and a client. Particular aspects of the service – quality, availability,

responsibilities–are agreed upon between the service provider and the service user. The most common component of an SLA is that the services should be provided to the customer as agreed upon in the contract.

Virtual Machine (VM): Virtual machine is the emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

14.2 General Guideline

The university's Data Centre may not be used in certain scenarios where the computing power needed to host application may not be available, in such cases cloud computing platforms may be utilized. Some major cloud providers have services like Email(Gmail), Storage and database which the University will have to use due to convenience and other reasons. In the preceding scenarios, UESD data may be stored in the cloud; this takes the responsibility of ensuring safekeeping of these data out of the hand of UESD staff to the external cloud providers.

The use of the cloud computing resource should comply with existing UESD data policies and the data protection act of Ghana. A staff member who uses any of these cloud services is responsible for ensuring that the confidentiality, integrity and availability of data and/or services is not compromised.

To ensure that this objective is achieved, Staff should:

1. Read and understand fully the Terms and conditions of Services offered by the cloud provider before accepting them. When accepted this binds UESD to a contract and therefore must be treated with care and clarifications sought when needed. seek expert opinions and advice before going ahead to store data or information on a computer not found in our on-premises data centre. This is to be done to ensure that everything is compliant with policies and legislation of UESD and the country as a whole

2. consult with the Director, DITSO for guidance.

3. make sure consultation with various stakeholders is well documented. This document can serve as a reference point when the need arises.

The following questions under the C.I.A. theme must be asked and also serve as a checklist for staff when choosing a cloud service provider

Confidentiality:

1. What intellectual property rights do the terms of use of the service grant to the service provider?
2. What rights are you signing away?
3. What measures does the service provider take to keep information confidential?
4. Is it possible to take down and delete information easily, quickly and permanently from servers or transfer it to a different provider?

Integrity:

1. What are the service provider's arrangements for protecting your data from unauthorized access, unauthorized amendment or deletion?
2. Do their guidelines provided adhere to institutional policy?
3. Do unauthorized exposures of university data result in the service provider notifying within the mutually agreed time of discovery?
4. Does the service provider comply with data retention and protection regulations and policies?

Availability:

1. Does the service provider make any performance guarantees?

2. Are the services and services levels adequate for your needs?

3. Does the external service provider have arrangements in place to ensure the long-term survival of the data?

14.3 Privacy and Data Security

1. Personal information and records that legislation does not allow to be stored outside of on-premises data centre or outside a geographical region must not be stored in the cloud since it may lead to a breach of such legislation

2. Staff should consult with Security experts, report and document issues where Privacy issues are unclear.It is the responsibility of the staff member storing the data to ensure that physical and logical security measures adequately protect the information being stored.

3. Information or data that has been marked as confidential, sensitive or secret may not be stored in such a way that the information or data could be accessed by any unauthorized parties.

4. Institutional information, staff information, or any other personally identifying information must be stored in a manner that fully protects the privacy of the individual and is fully compliant with all relevant and existing policies.

14.4 Records Retention and Availability

Information stored in the cloud must not only be kept secured but must also be available to authorized users when they need them to perform their duty. Data must be retained according to guidelines outlined by our record management policies.

14.5 Requirements of Cloud Services

Major cloud providers have SLA that defines in detail their service levels; this must be the first requirement to consider when engaging the service. The SLA in addition to a clear definition of services should address the following pain points.

1. agreed-upon service levels

2. clearly defined physical and logical security conditions

3. performance measurement

4. problem management

5. customer duties

6. disaster recovery

7. termination of agreement

8. protection of sensitive information and intellectual property

9. agreement of the disposal of information when required

10. definition of vendor versus customer responsibilities, especially on backups, incident response, and data recovery

The next requirement to consider should be ease of migration. Since data stored in the cloud may be needed elsewhere the provider must allow the export and use of data on our on-premise data centre or another provider. Service must allow for the permanent deletion of data. This flexibility allows you to discontinue the use of services and use different providers without losing your data.

14.6 Virtualization standards

The computing resource allocated to you by the cloud providers normally in the form of Virtual Machines and Containers should adhere to industry standards.

1. Hardened/Shielded VMS are virtual machines (VMs) fortified by a set of security controls that help defend against rootkits and bootkits.

2. Automatic patches and updates for a more secure server operating system environment.

3. Dedicated VMs to create a consistently configured environment that is secured against known vulnerabilities in the operating system and application software.

15.0 ICT ACCEPTABLE USE GUIDELINE

The ICT resources provided for academic purposes and University business are extremely valuable assets which are relied upon for the delivery of university services. This policy is designed to support all areas of the University's business and to recognize academic freedoms when using ICT resources. This policy will enable the University to carry out its activities, by protecting and preserving university ICT resources at the appropriate level. The policy is intended to protect the ICT assets of the University by adopting the core principles of information security:

1. Confidentiality – the prevention of unauthorized disclosure of information;
2. Integrity – the prevention of corruption or unauthorized amendment or deletion of information;
3. Availability – the prevention of unauthorized withholding of information or resources.

15.1 User Scope

This policy applies to people denoted as 'users' in this Policy, using the UESD ICT resources including, but not limited to:

1. Students enrolled at the University;
2. Applicants applying to the University;
3. Permanent staff employed by the University;
4. Temporary, casual or agency staff working for, or on behalf of the University;
5. Contractors, consultants and suppliers working for, or on behalf of the University;
6. Visitors to the University.

This policy applies to all users of UESD resources regardless of their role including, but not limited to: support roles, teaching roles, research roles and all student roles.

15.2 Resource Scope

This policy applies to ICT resources and systems made available for use by users or on behalf of UESD, including but not limited to:

1. PCs including desktop PCs, Apple Macs or other Apple computers, laptop PCs and terminals;

2. Peripherals e.g. printers, copiers and scanners;
3. Mobile devices, including smartphones, tablets, iPods, PDAs (Personal Digital Assistants), telephones, mobiles and other 'smart' devices;
4. Networks with wired, wireless or internet connections;
5. Internet services including the world wide web, blogs and wikis;
6. Email and other messaging, social networking or collaboration services e.g. blogs, chat, forums, Facebook, Twitter, YouTube, Instagram etc.;

15.3 General Guideline

When using ICT resources and engaging in digital communications such as email, instant messaging and video conferencing, users are expected to comply with the letter and the spirit of this policy and specifically:

1. must not access any information that are not permitted to be accessed.
2. must not use any ICT resource that are not permitted to be used.
3. must not display, store, transmit or knowingly receive images, text or any other material which could be considered illegal or defamatory
4. must not engage in behavior that damages or adversely affects any university ICT resources or damages or adversely affects the ability of other users of the University ICT resource.
5. must not use any ICT resource in a way that brings, or may bring, the University into disrepute.
6. must not compromise or risk compromising the security, confidentiality, availability or integrity of the University's ICT resources in any way whatsoever
7. must ONLY enter (or direct others to enter) Credit/Debit card numbers and associated security codes into approved PCI-DSS compliant payment collection devices, e.g. approved tills and PDQ devices, or approved online payment collection applications and web interfaces using secure and approved computers. Credit/Debit card numbers and associated security codes should NEVER be written down on paper, typed into emails, stored in spread sheets or other documents, or entered into non approved ICT PCI-DSS systems or devices. If you do receive an email containing a Credit or Debit card number, you must delete it immediately.
8. must take appropriate care when using sensitive data and abide by all relevant data protection legislation including the General Data Protection Regulation (GDPR).
9. must not knowingly introduce malicious software, such as viruses or similar threats, into any university ICT resource or other ICT resource.
10. must not use any ICT resource in contravention of any applicable license agreements or copyright obligations.
11. must not use another user's identity or otherwise disguise their, or your own identity when using any ICT resource. You must only use your assigned account username and password to access university ICT resources; the password must comply with the password policy.

16.0 ICT TRAINING GUIDELINE

16.1 Scope

1. This Policy applies to all training of systems and IT competencies that will require any form of assistance from DITSO. This Policy only applies to training that is under the jurisdiction and knowledge of DITSO. All UESD employees are expected to adhere to this policy.

Objective

The broad goals of this policy are:

Establish IT training through an identified need

Prevent the implementation/rollout of systems without the necessary training

16.2 General Guideline

1. Training Equipment:

2. All training equipment should not be personalized in terms of setting individual passwords and making unauthorized installations of software.

3. Training materials

Any training material used are the property of UESD and should not be shared outside the University fraternity. They should be kept confidentially in the custody of the person in charge of the IT library.

   a. Training will be performed on a basis deemed necessary to guarantee the effective support of IT systems.

   b. The training shall be approved by the Director, DITSO and/or the requisite line manager.

   c. For effective IT assistance on any system, there shall be the need for insistence on a training that is beyond the level of a Seminar that occurred for more than a single day.

4. Training durations shall be recognized as follows:

   a. Day (couple of hours)

b. Day (Morning/Afternoon session).

c. Days (More than 1 day).

d. Weeks (More than 1 week).

e. Months (More than 1 month).

5. It is the responsibility of the Director, DITSO and his/her unit heads to keep track of the training schedule at least once per month. It is also their responsibility to provide evidence of successful completion to the Vice Chancellor at least once per quarter.

16.3 Disclaimer

DITSO shall not be held liable for any IT systems deployed without their prior knowledge or training. Deliberate and serious breach of these policy statements in this section will lead to disciplinary measures which may include the offender being denied access to computing facilities.

17.0 ASSET MANAGEMENT GUIDELINE

This guideline describes the asset management procedure to be used by UESD. It provides the overall framework for management of IT equipment. These policy statements shall apply to all the distinct phases in the entire physical life cycle of all ICT assets: Planning, Acquisition, Operation and Disposal.

17.1 Scope

This guideline applies to all staff and students of UESD who use IT equipment purchased by the University including:

1. All desktop and laptop PCs;
2. All printers, copiers and scanners;
3. All phones, mobile phones and smartphones;
4. All servers, network switches etc.;
5. Any other IT peripheral.

17.2 Objectives

1. Improve ICT service provision through asset control;
2. Improve financial planning through identification of ICT assets and allocations;
3. Improve software license management and legal compliance;
4. Increase confidence in ICT systems and service delivery;
5. Increase user satisfaction.

17.3 Responsibility and Authority

It is the responsibility of the Heads of Units and Departments to monitor the use of this policy, and to report violations to the Disciplinary Committee of the University. It is the responsibility of the Director, DITSO to verify the practices and procedures for effective use and to execute corrective measures when appropriate.

17.4 General Guidelines

1. All ICT hardware equipment must be procured through DITSO;
2. Any request for new equipment must be given to DITSO for verification and written recommendations with specifications forwarded to the VC for approval/disapproval;
3. Departments other than ICT are specifically prohibited from purchasing any of the following equipment:

    a. Desktop and laptop PCs, monitors, printers, scanners, phones, digital cameras, storage and removable devices;

    b. Hardware asset tags will be affixed to PCs and laptops on receipt by stores before distribution. These tags will identify the asset with a unique asset number. A continually-running inventory system will be used to maintain a register of PCs and laptops, and the software installed on them by DITSO. This audit information will be checked at least twice yearly against the License Dashboard to ensure that there is a match between software installed and software licenses owned.

    c. Accurate, updated and maintained inventory shall be kept for all ICT equipment at DITSO;

    d. All ICT equipment shall be signed for (without amendment) by equipment holders and declaration scanned into the inventory management system;

    e. Reports on any assets stripped for spare parts shall be documented and removed components noted within the asset management system. Data on harvested drives will immediately have their data archived using a method approved by DITSO;

    f. All unwanted/redundant ICT related assets are to be disposed of by DITSO, in accordance with the appropriate procedure prescribed by the Directorate of Audit;

    g. After purchase all new ICT equipment should be inspected and certified by DITSO before issuance by Stores;

    h. Before issuance all equipment shall be tagged and referenced in the system;

    i. Any Loss or theft of ICT equipment must be reported immediately to DITSO;

    j. All ICT equipment (including portable devices) must be returned to Stores upon replacement, equipment redundancy or when the holder loses affiliation to the University;

    k. Equipment holders will retain responsibility for equipment issued to them until it has been returned to DITSO for redeployment or disposal;

    l. It is the responsibility of DITSO and the respective Head of Unit or Department to ensure that ICT assets are replaced according to the procedures prescribed below. It is imperative that any replacement performed by the University be done appropriately, responsibly, and ethically with resource planning in mind. The following rules must therefore be observed:

        i. Obsolete IT Assets: “Obsolete” refers to any and all computer or computer related equipment over 3 years old and/or equipment that no longer meets

requisite functionality. Identifying and classifying IT assets as obsolete is the sole prerogative of the ICT Committee. Decisions on this matter will be made according to the UESD procurement strategies. Equipment lifecycles shall be determined by ICT asset management best practices (i.e. total cost of ownership, required upgrades, etc.);

ii. Reassignment of Retired Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of DITSO. It is, however, the goal of the University to, whenever possible to reassign ICT assets in order to achieve

iii. full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function is appropriate;Trade-Ins: Where applicable, cases in which an equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old ICT asset against the cost of the replacement. The Head of the Procurement Unit and the Director, DITSO shall assume this responsibility;

4. Cannibalization and Assets beyond Reasonable Repair: The Director, DITSO is responsible for verifying and classifying any ICT asset beyond reasonable repair. Equipment identified as such shall be cannibalized for any spare and/or working parts that can still be put to sufficient use within the University. DITSO shall take inventory and stockpile these parts in collaboration with Stores. The remaining parts and/or whole machines unfit for use or any other disposal means shall be subject to the University's disposal procedures.

17.5 ICT Asset Disposal Procedure

1. The Director, DITSO reports of unserviceable or obsolete equipment to the ICT Committee;

2. The ICT Committee shall recommend a method of disposing of the equipment which may include any of the following:

   a. transfer to another public entity with or without financial adjustment;

   b. sale by public tender/auction;

   c. destruction by dumping or burying;

3. Within the prescribed time period after receiving the recommendations from the ICT Committee the Head, Procurement Unit shall give a written notice as to whether he/she accepts or rejects the recommendations of the committee;

4. If the Head, Procurement Unit accepts the recommendations, the equipment shall be disposed of in accordance with the recommendations. The disposed item shall be indicated in the inventory that it has been disposed of;

5. If the Head, Procurement Unit rejects the recommendations of the ICT Committee he/she shall include with the notice given, written reasons for rejecting the recommendations and refer the matter back to the Committee for further consideration.

17.6 Consequences

- Misuse or abuse of ICT assets through violation of this policy shall result in disciplinary action and/or surrender of equipment.

18.0 GUIDELINES ON AI USE AND ACADEMIC INTEGRITY

This guidelines establishes clear guidelines for the ethical and responsible use of Artificial Intelligence (AI) at the University of Environment and Sustainable Development (UESD). As AI becomes more integrated into academic and professional environments, UESD recognizes the need for structured regulations to ensure AI usage aligns with the University's principles of academic integrity, equity, and sustainability. The policy defines expectations for students and faculty regarding AI's role in teaching, learning, research, and assessment.

This guideline promotes the ethical and appropriate use of AI tools in academic activities while maintaining UESD's commitment to transformative learning and academic integrity. It recognizes assessment as a core component of the teaching-learning process and provides guidance for lecturers on integrating AI into education, as well as recommendations for students on its responsible use. These guidelines are particularly relevant to invigilated summative assessments within academic modules.

This policy is guided by two key principles: (1) the ethical and responsible use of AI in generating academic work and (2) the innovative application of AI in teaching, learning, and assessment. While the primary focus is on ensuring responsible AI usage, UESD also provides ongoing training and professional development to support its integration into pedagogy. The policy applies to generative AI tools such as ChatGPT, Bard, and DALL-E, emphasizing the importance of educating graduates on their ethical application.

This policy aligns with existing UESD regulations, Ghanaian educational standards, and national laws such as the Data Protection Act, 2012 (Act 843) and the Criminal Offences Act, 1960 (Act 29). By adhering to these frameworks, UESD ensures that assessments remain transparent, fair, and reflective of genuine student learning and progress.

This policy defines three primary AI usage scenarios:

1. Permitted AI Use, where students may use AI for idea generation and language enhancement but must critically assess and disclose its impact.

2. Prohibited AI Use, where AI is banned in assessments requiring independent analysis and comprehension; and

3. Required AI Use, where AI is mandated for specific assignments, with clear ethical guidelines and alternative provisions for students who may not have access to AI tools. Unauthorized AI use is classified as academic misconduct and will be subject to disciplinary measures.

This policy requires that AI regulations be clearly communicated within course syllabi and

assessment guidelines. Both students and lecturers must declare AI usage, specifying the tools and their application. A student declaration form is included, ensuring that AI-generated content maintains originality and academic integrity.

This policy also recommends that students document their AI interactions by preserving prompts and responses to maintain transparency in academic work. By implementing these structured guidelines, UESD ensures that AI serves as a tool to enhance learning rather than replace critical thinking and independent scholarship.

18.1 Institutional Guidelines for Responsible AI Use in Academia

These institutional guidelines define UESD's approach to the responsible use of AI tools in academic settings. Any faculty-specific guidelines must align with theseoverarching principles, which will be reviewed and updated annually to reflect ongoing AI advancements. The guidelines offer two perspectives, guidance for:

1. lecturers on adapting teaching practices to support students in an AI-driven world, and
2. students on using AI responsibly to enhance both immediate and long-term learning.

Rooted in a student-centered approach, this policy promotes academic integrity while fostering AI literacy as a collaborative learning process.

The recommendations emphasize ethical AI use in alignment with UESD's Code of Conduct and academic misconduct policies. Rather than viewing compliance as a mere obligation, students and staff are encouraged to see responsible AI use as a means of academic and professional growth. Key terms include:

1. Declaration (a signed statement disclosing AI use).
2. Reference/Citation (proper attribution of AI-generated work).
3. Original/Individual-Created Content (work produced solely by an individual without AI assistance).
4. AI-Generated Content (work predominantly created using AI, with users accountable for its integrity).

18.2 Ethical Framework

18.2.1 Preparation for an AI-Driven World

1. UESD equips graduates to engage with AI technologies ethically and responsibly.
2. These guidelines establish a framework to uphold academic integrity amidst technological advancements.
3. Key supporting policies:
    a. Academic Integrity Policy
    b. Teaching and Learning Policy

18.2.2 Teaching and Learning Policy

1. Focuses on student preparedness for a dynamic global environment.
2. Emphasizes education as a responsibility requiring accountability.
3. Aims to develop ethical principles and professional competencies.

18.2.3 Academic Integrity Policy & Assessment Policy

1. Require transparent and fair assessment processes.
2. Emphasize the production of original work.
3. Prohibit academic dishonesty, including plagiarism.
4. Ensure integrity and transparency in all academic activities.
5. Promote fairness in evaluations, fostering genuine student engagement.

18.2.4 Student Code of Conduct

1. Establishes procedures for handling academic misconduct in terms of:
    a. Plagiarism – Using another person's work without proper attribution.
    b. Self-Plagiarism – Reusing one's own prior work without citation.
    c. AI-Assisted Plagiarism ("AIgiarism") – Inappropriate AI use undermining academic integrity.
2. Reinforces that AI tools should not replace personal accountability in learning.

18.2.5 Compliance with National Standards

1. GTEC Quality Assurance Framework – Ensures academic quality in higher education.
2. Data Protection Act, 2012 (Act 843) – Regulates ethical data use, crucial for AI interactions.
3. Criminal Offences Act, 1960 (Act 29) – Addresses fraud, forgery, and identity misrepresentation, including AI-related misconduct.

18.2.6 Commitment to Ethical AI Use in Teaching, Learning, and Assessment (TLA)

1. Academic integrity entails intellectual honesty, avoiding:
    a. Plagiarism
    b. Self-plagiarism
    c. Cheating

2. Collusion
3. Fabrication
4. Unethical AI use

2. UESD's approach to AI in TLA must align with these principles.

18.2.7 Institutional Support for Responsible AI Use

1. UESD fosters ethical AI engagement for students and faculty.
2. Encourages transformative learning while ensuring integrity and accountability.
3. Prepares students to ethically navigate a technology-driven world.

18.3 Core Principles for Practice

These principles provide a foundation for ethical AI integration in education, reinforcing UESD's commitment to student-centred learning and academic integrity.

18.3.1 Accountability

1. Ensures proper acknowledgement of sources and attribution of AI-generated content.
    a. Ideas are shaped by others' contributions, requiring proper referencing and citation.
    b. UESD follows the Academic Integrity Policy to ensure appropriate attribution.
2. Ensures responsibility for accuracy and integrity
    a. Authors must ensure their content is factual, ethical, and free from harm.
    b. AI tools lack accountability; users must critically assess AI-generated content.
    c. Avoid disseminating misinformation or sharing personal data.
3. Ensures AI-Generated Content are verified
    a. AI does not create original ideas but relies on existing datasets.
    b. AI cannot be cited as an author of any academic work.
    c. Users must:
        i. Assess and validate AI-generated material for accuracy and relevance.
        ii. Properly attribute sources in line with UESD's referencing guidelines.
4. Some AI tools (e.g., Bard) provide source links, but users must verify their academic reliability.

18.3.1. Responsibilities of Lecturers in AI Utilisation

1. Educate Students on AI Usage
    a. Explain appropriate AI use, including when it is prohibited and why.
2. Demonstrate Responsible AI Use
    a. Maintain transparency about personal AI usage in teaching.
    b. Serve as a model for ethical AI integration.
3. Facilitate Ethical Discussions
    a. Encourage open discussions on AI ethics, biases, and societal impacts.
4. Ensure Accuracy and Safety
    a. Verify that AI-generated content used in teaching is factual.
    b. Prevent the spread of misinformation or personal data breaches.

18.3.1. Responsibilities of Students in AI Utilisation

1. Accountability for Submitted Work
    a. You are responsible for the accuracy and integrity of your work.
    b. Ensure your submissions do not cause harm or mislead others.
2. Critical Assessment of AI Outputs
    a. AI lacks accountability: you must verify all AI-generated content.
    b. Avoid spreading misinformation, misappropriating content, or revealing personal data.

18.3.2 Authenticity

Promotes genuine student engagement and original work.

1. Ensuring Genuine Student Learning
    a. Lecturers must confirm that assessed work reflects the student's own effort.
    b. Assessment should accurately measure the student's attainment of learning outcomes.
2. Original Contribution
    a. Students must clearly distinguish their original work from external contributions.
    b. Prior work by the student should be properly referenced to demonstrate new insights.
3. Declaration of AI Use
    a. Students must disclose the AI tools used and specify their application in their

work.

b. Justification must be provided to confirm that the work remains authentically their own.

18.3.2. Lecturer Responsibilities in Ensuring Authenticity

1. Design AI-Resilient Assessments
    a. Develop assessments that minimize reliance on AI or ensure AI use does not overshadow student understanding.
2. Maintain Student Authorship
    a. Implement strategies that verify the student's authentic contribution to their work.
3. Establish Clear AI Guidelines
    a. Define explicit rules on when and how AI may be used in each assessment.
4. Engage in Continuous Professional Development
    a. Utilize available resources and training to integrate AI responsibly in teaching and assessment.

18.3.2.b Student Responsibilities in Ensuring Authenticity

1. Understand Assessment Requirements
    a. Clarify AI usage guidelines for each task. Assume AI is prohibited unless explicitly allowed.
2. Maintain Independent Learning
    a. Use AI as a supportive tool, not as a substitute for personal effort and comprehension.
3. Critically Engage with AI Content
    a. Ensure AI-generated output aligns with your own understanding and voice. Be prepared to justify your work by:
    b. Answering detailed questions or explaining choices in an oral assessment.
    c. Summarizing key ideas independently and demonstrating comprehension.

18.3.3 Fairness

Maintains equitable teaching, learning, and assessment (TLA) practices.

1. Equal Opportunity in Assessment
    a. All students must have a fair chance to succeed.
    b. AI-related irregularities should be handled responsibly, considering the challenges of verification.

2. Avoiding Unfair Advantage
3. Submitting AI-generated work as one's own creates an unfair advantage.
4. This can affect important decisions like admissions, scholarships, and academic rewards
5. This can affect important decisions like admissions, scholarships, and academic rewards.

18.3.3.a Lecturer Guidelines for Fair AI Use

1. Design AI-Resistant Assessments
    a. Use project-based tasks, open-ended questions, or oral assessments to minimize AI misuse.
2. Holistic Evaluation
    a. Consider multiple sources of information for decisions on admissions, awards, and academic progression.
3. Ensure Fairness and Accessibility
    a. Be mindful of students' varying digital skills and access to AI tools.
4. Provide Alternative Options
    a. No student should be forced to register for AI tools; alternatives should be available.
5. Promote Ethical AI Use
    a. Discuss fairness and integrity in AI use to ensure equitable evaluation.

18.3.3.b Student Guidelines for Fair AI Use

1. Adhere to Ethical AI Practices
    a. Follow UESD's academic integrity standards and avoid using AI in ways that misrepresent your abilities or generate inaccurate content.
2. Demonstrate Your Understanding
    a. Be ready to explain your thought process, methodology, and conclusions to show genuine comprehension.
3. Develop Independent Skills
    a. Avoid over-reliance on AI, as it may hinder your ability to succeed in future assessments that require independent problem-solving and critical thinking.

18.3.4 Transparency

Clarifies the distinction between human effort and AI-generated contributions.

1. Clear Assessment Requirements
    a. UESD ensures that students receive detailed, transparent information about assessment criteria and evaluation methods.AI Use Declaration
    b. Students should declare their use of AI in assignments, specifying how and where it was applied, to avoid academic misconduct and address concerns about plagiarism or "AIgiarism."

18.3.4.a Lecturer Guidelines for Transparency in AI Use

1. Communicate AI Guidelines
    a. Clearly explain the rules for AI use, ensuring students understand when and how AI tools can be applied in their work.
2. Specify AI Use in Assessments
    a. Detail how AI tools will be incorporated into assessments, including their intended purpose and any limitations.
3. Ensure Data Protection
    a. Adhere to UESD's data protection policies and ensure no personal or confidential student information is entered into AI systems.
4. Consider Metadata
    a. Be mindful that AI platforms may collect metadata (e.g., device information, interaction patterns), even with chat history disabled, and be cautious of how this data might be used.
5. Inform Students About Privacy
    a. If AI use is allowed or required, inform students about potential privacy risks and encourage caution when using AI tools.

18.3.4.b Student Guidelines for Transparency in AI Use

1. Declare AI Use
    a. Honestly and transparently declare the use of AI tools, including specifying the tool, extent of its use, and the purpose behind it. Reflect on why the AI approach was suitable and any potential limitations of this choice.
2. Review Privacy Settings
    a. Carefully review the privacy settings of any AI tools you use to understand what data is being collected and how it may be used, as explained in the application's Terms and Conditions upon registration.

18.4 AI Use Declaration and Integrity Guidelines

UESD encourages students to transparently declare their use of generative AI tools by detailing specific tasks, such as outlining, idea generation, or proofreading. Students should document AI interactions, including prompts and outputs, and submit them

with their assignments. They must also accept responsibility for any errors, copyright issues, or plagiarism introduced by AI. Rather than banning AI usage, UESD promotes academic integrity through transparency. Any misconduct related to AI use declarations will be addressed according to UESD's standard procedures for handling academic dishonesty.

18.4.1 Approaches to AI Use at UESD

1. Encourage Responsible Use of Declarations: UESD promotes the responsible use of AI by ensuring transparency and adherence to declaration protocols, as outlined in these guidelines.

2. Prohibit AI Use Where Appropriate: Certain departments or lecturers may choose to prohibit AI tools for specific assignments. However, safeguarding assessments from AI-generated content is difficult, and unreliable AI detection tools may inadvertently penalize honest students, affecting fairness, especially in postgraduate admissions and funding.

3. Require AI Use with Accountability Measures: In some cases, UESD may require the use of AI for specific tasks, with students following declaration standards. Alternatives will be provided for students who wish to opt out due to privacy concerns related to AI tool registration requirements.

18.4.2 Permissible AI Use at UESD

1. UESD follows the practices of publishing houses and academic institutions regarding the use of tools and sources in knowledge work.

2. The principles in 18.3 apply to all types of academic and creative work, including:

    a. Research papers

    b. Artwork

    c. Codes

18.4.3 Student Use of Generative AI Tools

1. UESD fosters a student-centred learning environment that emphasizes responsible AI use based on core the principles enumerated in 18.3 above.

2. The table below provides guidance on how different types of AI usage impact learning, linking AI-use scenarios with common academic practices and suggesting actions for responsible engagement. This helps students maximize learning while maintaining academic integrity and adhering to UESD's standards.

Table 18.1 AI-use Guidelines

AI use for	Academic Practice	What the use is like	What to remember to do
Brainstorming Topics or Approaches. E.g., Using AI to help you generate ideas or narrow down a topic for your paper.	Idea generation phase of an assignment	Engaging in a discussion with a friend, tutor, or teacher about the idea.	It could be helpful to document the prompts you used and the responses you got.
Formulating an outline or blueprint.		Conducting an online search or consulting Wikipedia.	Critically review the outline suggested by the AI, ensuring it aligns with your assignment's requirements and goals. Edit as needed so it fully represents your own thinking and approach. You should assess the AI output thoughtfully and verify its accuracy
Researching/ Gaining knowledge on a specific subject E.g., Using AI to gather background information on a topic.	Revision Phase of an assignment	Conducting an online search on Google or consulting Wikipedia.	It's important to (1) identify and cite original sources if using the information in your work and (2) confirm that the content is factually accurate and won't cause harm by spreading misinformation or disclosing personal details.

Literature Review and Finding Sources. E.g., Asking AI to suggest books, articles, or papers relevant to your topic.		Using an academic database like JSTOR or Google Scholar	Always verify that any sources suggested by AI exist, are credible, and are relevant to your topic. AI tools may sometimes fabricate citations or suggest unreliable sources. If in doubt, rely on UESD's library databases for authentic materials.
Drafting Text or Generating Content. E.g., Using AI to generate a paragraph or to help structure an argument.		Ask someone to write parts of your paper for you (not permitted for academic integrity).	If you use AI to draft parts of your work, make sure you thoroughly understand and can explain any AI-generated content.This content should serve only as a starting point or guide. Revise it significantly to reflect your perspective and insights, or otherwise, it may be considered misrepresenting your abilities

18.4.3. AI Use Declaration

1. To ensure transparency and ethical use, all students must complete the AI Use Declaration form for any work involving AI assistance.
2. The declaration, to be included with the assignment submission, must outline the following:
    a. The specific AI tools used in the work.
    b. The scope and purpose of AI assistance (e.g., idea generation, outlining, proofreading).
    c. A statement affirming the student's responsibility for the work and acknowledging any potential issues such as errors, plagiarism, or copyright concerns arising from the use of AI tools.
    d. Documentation of AI interactions (e.g., screenshots or records of prompts and outputs) must state:
        i. The specific AI tool(s) used (e.g., ChatGPT, Midjourney, Meta AI, Quillbot, etc.)
        ii. The purpose and extent of involvement within the work: (e.g., generating an outline, fact checking, language editing)

iii. The Justification affirming that the work genuinely represents the student's knowledge and contributions, and how they ensured it aligns with academic integrity standards.

Table 18.2: AI use declaration Form

The specific AI system(s) used	Why was it used?	What was it used for? / where in the work was it used?
To what extent did you use AI?		
Why do you consider that the work is your own?		

18.4.3.b AI Use Checklist

1. Confirm work reflects personal learning, skills, and understanding, and can support this claim.
2. Acknowledge the need to declare AI tool use if used to enhance ideas or writing.
3. Declare and document AI tool use for generating ideas, wording, code, or image prompts, and be ready to explain its contribution.
4. Understand that lecturers may request further demonstrations of understanding, such as oral assessments.
5. Confirm that AI tools were not used if explicitly prohibited.
6. Acknowledge that failure to comply with these statements may lead to academic misconduct and the penalty thereof shall be applied.
7. Take responsibility for the integrity of work, seeking clarification from academic staff when uncertain.
8. Understand that unauthorized AI tool use or failure to declare may violate academic integrity standards and lead to disciplinary action.

18.4.3.c Required Documentation

1. Students are encouraged to document their use of AI tools, including:
    a. Prompts used.
    b. Conversation snapshots.
2. This documentation provides transparency and can be reviewed if necessary.

18.4.4 Lecturer Use and Response to Generative AI Tools

1. Lecturer use of AI at UESD involves integrating AI tools into teaching, learning, and

assessment practices.

2. It also includes guidance on what AI tools are allowed and encouraged for student use in academic work.

3. The following recommendations apply to both lecturer usage and student engagement with AI tools.

18.4.4.a Lecturer AI Use Guidelines

1. Equitable Access: AI tools should be used fairly, considering students' access to these technologies.

2. Clarity in AI Use Policies: Clearly define when AI use is allowed or prohibited and what constitutes academic integrity breaches. This should be communicated

through classroom discussions, module frameworks, assignment instructions, and assessment rubrics.

3. Accessibility of Policies and Consequences: Ensure AI policies and consequences are fully accessible and consistently communicated to students.

4. AI Use in Assessing Student Work:

a. AI tools like ChatGPT or Quillbot may assist lecturers in reviewing assessments but should not fully replace human review.

b. Lecturers must verify AI-generated outputs for accuracy and ensure agreement with their own assessments.

c. Personal or sensitive student information should not be shared with external AI systems.

d. Declare which AI tools will be used, how they will be applied, and how student queries and AI outputs will be verified or moderated.

e. AI detection tools may yield false results and should not be solely relied upon to determine academic misconduct.

18.4.4.b Lecturer AI Use Checklist

1. Awareness of AI's Impact on Assessments: Understand the potential impact of generative AI on the structure and integrity of assessments.
2. Assessment Redesign: Consider adapting or redesigning assessments to account for AI use where appropriate.
3. Clear AI Usage Policy: Decide whether to allow responsible AI use with mandatory student declarations or to prohibit AI use for specific assessments.
4. Communication of AI Policies: Communicate AI usage policies to students in line with UESD's guidelines.
5. Transparency in AI Use for Assessment: Inform students if AI tools will be used in the assessment process.
6. Understanding the Limits of AI Detection: Recognize that AI detection tools may be unreliable, and use them only as supplementary indicators. Any suspicions of AI-generated content should be carefully reviewed to ensure fairness.

18.4.5 Risks of Overreliance on AI

1. Excessive use of AI for tasks beyond assistance, such as generating entire essays, can hinder learning and preparedness.
2. UESD encourages students to use AI as a tool to enhance learning, not as a replacement for critical thinking.

18.5 Addressing AI Misuse and Academic Integrity

1. Academic Integrity Foundation: UESD's academic activities are based on values of academic rigor, honesty, and trust, which form the core of academic integrity.
2. Academic Misconduct Prohibition: Academic misconduct, such as plagiarism and falsification of data, undermines these values and is strictly prohibited.
3. Student Disciplinary Code: UESD's Student Disciplinary Code addresses academic misconduct, with penalties potentially affecting students' academic records, final grades, or assessment results.
4. AI Misuse: When AI misuse is suspected, appropriate measures will be taken according to UESD's academic integrity policies.
5. When AI misuse is suspected:
    a. Initial review: The instructor will schedule a discussion with the student, outlining concerns and reviewing the submitted work, as well as clarifying AI policies
    b. Evidence submission/Documentation review: The student should provide relevant AI interaction records and declaration forms
    c. Follow-Up Actions:
        i. If AI misuse is confirmed, the case may lead to disciplinary action per UESD's Code of Conduct.
        ii. First offenses may involve a warning and learning support, while repeated infractions could lead to stricter consequences.

18.5.1 Procedures for Managing Suspected Misuse

1. Initial Contact: The student will be contacted via email to discuss concerns regarding their submitted work.
2. Pre-Meeting Information: Before the meeting, the student will receive:
    a. A clear statement of the allegations.
    b. Details of the specific work under review.
    c. A marked-up version of the work indicating the areas of concern.
3. Student Preparation: The student should bring:
    a. Their declaration of AI use.
    b. Relevant evidence such as AI chat history or prompts used.
4. Discussion Opportunity: During the meeting, the student can:
    a. Explain how, why, and to what extent they used AI in the work.
    b. Answer questions about the content and context of their submission to clarify their understanding and role in the work.

18.5.2 Impact on Grades

1. Confirmed Irregularities: May result in a grade reduction or no credit for the affected assignment or assessment.
2. Decision Authority: Faculty discretion and academic integrity policies will determine the penalty.
3. Purpose: Ensures fairness and upholds UESD's academic standards.

18.5.3 Remedial Measures Summary:

1. Educational Approach: UESD prioritizes fostering an understanding of AI ethics over harsh penalties for first-time offenses.
2. First-Time Offenses: Discussions should focus on learning, guidance, and correction rather than strict punishment.

18.6 Commitment to Continuous Improvement and Support

1. Ongoing Review: UESD will continuously update guidelines to align with AI advancements.
2. Support Resources: The University will provide workshops, tutorials, and educational materials to help students and faculty use AI ethically and effectively.
3. Fostering Integrity: These guidelines aim to promote AI as a tool for learning and innovation while upholding integrity, accountability, and fairness.