CHISONA ACADEMY

Embrace the Achiever in You

Staff ICT Policy

Updated	01 September 2023
Reviewed Date	01 August 2024
Authorised by	Emmanuel C AJOKU

OBJECTIVE

The objective of this policy is to ensure effective use of Chisona Academy`s Information Technology (IT) resources, website, learning platform and protect the organisation from deliberate or accidental misuse of organisation equipment or systems.

PURPOSE

The purpose of this document is to communicate the policies and procedures with which individuals must comply to ensure an appropriate level of security within the organisation. This includes:

- Ensuring all users with access to IT facilities are aware of the principles of the appropriate use of these facilities.
- Ensuring all use of the organisation facilities complies with relevant legislation.
- Ensuring that IT facilities are used for authorised purposes; and
- Making users aware that they may be denied access to IT facilities or subject to further action if they are not in compliance with the policy.

The policy has been developed broadly in line with the best practice guidelines for Information Security Management as set out in ISO 27001/2.

AIMS

Information security covers the protection of all forms of information to ensure its confidentiality, integrity, and availability.

We seek to preserve:

- **Confidentiality**: data and information can only be seen by those authorised to see it and can only be amended by those allowed to amend it.
- **Integrity**: the data is complete, accurate, up to date and relevant and the system is operating as per the specification.
- **Availability**: information and services are delivered to the right person at the time and place they are needed.
- **Accountability**: all activity can be traced back to the originator.

This policy applies to all users of any equipment that is connected to the organisation network or used on a stand-alone basis, whether on a permanent or on a temporary basis. This includes organisation pupils and staff (permanent, temporary, or casual) and all other persons such as consultants, temporary staff or subcontractors who are granted access to organisation information and IT facilities. The policy applies to all data stored within any IT system or facility, which is managed under the control of the organisation.

We will attempt to ensure that:

- Information will be protected against unauthorised access.
- Regulatory and legislative requirements will be met.
- Business continuity plans will be produced, maintained and tested.
- Breaches of information security will be reported and investigated by the appropriate staff.
- Computer systems are used to enable the organisation to meet its vision.
- The aims of the security strategy are supported.
- The IT system promotes effective teaching and learning and contributes to the efficient administration of the organisation.

SCOPE

Included within the scope of this document are organisation policies for:

- General IT Usage
- Network Access and Computer Usage
- User Accounts and Passwords (Access Controls)
- Physical Security
- Portable Computers
- organisation Servers
- Virus Protection
- Backup and Maintenance
- E-Mail
- Internet Access

COMPLIANCE

It is the responsibility of all organisation staff and students to adhere to this policy along with all other associated security and data protection policies. Failure to comply will lead to the removal of access to IT facilities and may result in further action. Note that violation of certain aspects of this policy may also constitute a criminal offence.

If you are in doubt about any aspect of this policy, you must seek clarification from the organisation IT Technical Support team.

Policy Area: General IT Usage

Policy Objective

To establish general rules of good conduct in the use of IT resources and to make the IT systems a safe and secure place for all users.

Note

All users must read and accept the terms of the organisation Acceptable Use Policy – signing this policy indicates acceptance and agreement to be bound by its terms.

Do

- Ensure that you comply with the CHISONA ACADEMY Information and Data Protection policy, if in doubt; do not store details of identifiable individuals on any computer.
- Look after the facilities for the benefit of yourself and future users.

Don't

- Use organisation computing facilities to produce, obtain, store, display or distribute material that is likely to cause offence to others or is illegal.
- Deliberately or carelessly seek to delete, transmit or in any way access or modify another user's data. Please respect privacy.
- Copy or in any way distribute organisation software or data. Users are subject to the CHISONA ACADEMY organisation Copyright policy.
- Eat or drink in any designated IT area.
- Use the IT facilities to play computer games or download gaming software.
- Deliberately seek to circumvent the organisation IT security systems.

Policy Area: Network Access and Computer Usage

Policy Objective

To ensure that networked resources are used in an appropriate way and that users are allocated rights and responsibilities in network use.

Note

Students will be given access to the organisation network for the duration of their course. On appointment all staff will be given the appropriate level of access to the network to allow them to do their job. Authorised users will be issued with a username and a password.

Do

- Remember that the organisation reserves the right to monitor usage of its computing facilities, in order to ensure their proper, efficient, and legal use. Such monitoring will be undertaken on a regular basis. Users are warned that activities such as Web site access are subject to monitoring.
- Report any faults with IT equipment or software to the organisation IT Technical Support team.
- Be considerate in the use of shared resources.

Don't

- Leave PCs, laptops, and workstations unattended and logged on.
- Install unauthorised software on any organisation computers.
- Cause any form of damage to the organisation computing equipment, nor to any of the rooms and their facilities and services that contain that equipment or software. The term "damage" includes modifications to hardware or software that, whilst not permanently harming the hardware or software, incur time and/or cost in restoring the system to its original state.
- Move or remove any IT equipment, hardware, or software without prior agreement from the TCT Team, in accordance with current technical guidelines.
- Connect any device into the organisation IT network without prior agreement from the TCT Team, in accordance with current technical guidelines.
- Use organisation computing facilities to abuse or harass anyone, whether or not they are members of the organisation.
- Use the organisation IT systems to obtain personal financial or commercial gain.
- Deliberately waste time or resources to the detriment of other users or the environment.

Policy Area: User Accounts & Passwords (Access Controls)

Policy Objective
To ensure that all organisation systems and data are protected by robust logical access controls (passwords) and that users are aware of their responsibilities for password security.

Passwords

The IT Technical Support team will use organisation systems to enforce the provisions of this policy in relation to user accounts. It is the responsibility of all users to take the appropriate steps in selecting and securing their personal passwords.

All passwords will adhere to the following:

- Personal passwords must not be disclosed or shared.
- All accounts will be locked after 3 consecutive failed login attempts.
- Generic passwords will be created for new users and the user will be prompted during their initial login to change their password before proceeding. The generic password will be conveyed only to the new employee or to a supervisor or tutor.
- After a specified period of inactivity, the desktop/laptop will time-out and will be inaccessible until the user has logged back onto the system with a valid password.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- The use of password 'cracking' tools is prohibited.
- A valid proof of identity is required if you request your user password is to be reset.

IT Technical Support staff only

- All system-level passwords must be changed from the default delivered password.
- Super user accounts i.e. those that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Best Practice Password guidelines

'Strong' passwords should have the following characteristics:

- Must have a minimum 8 digits as well as letters.
- Are at least 8 alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.
- Changed frequently (every 30 days)
- Changed immediately if it suspected people other than the rightful owner are aware of the password. The organisation reserves the right to disable the

account or to force a password change in these circumstances.

Don't

- Attempt to connect to the organisation IT systems using anything other than your assigned user ID.
- Leave details in public view that would give rise to someone detecting your password.
- Use the 'Save Password' options in login boxes.
- Allow anyone else to log into the system using your user ID. You will be responsible for anything that is done whilst someone else is logged in under your account.

Policy Area: Physical Security

Policy Objective
To ensure that all organisation access to organisation premises, systems and data are appropriately physically secure and that users are aware of their responsibilities for site security.

General Site Security All

users
All users shall ensure that equipment is kept secure.
Shall speak to a member of staff if they suspect there is an unauthorised visitor on site
Shall speak to a member of staff if they think that there is a risk of equipment loss or damage.

All Staff
All staff should ensure that:

- All visitors sign in at Reception and are issued with a Visitors badge.
- Offices are not left unattended where possible during normal working hours.
- All computers in vulnerable areas (e.g., ground floor rooms) are physically secure.

Computer Room Security - IT Technical Support staff only

The security of the equipment in the computer rooms is vitally important to the operation of the organisation. Servers, networking, and telecommunications hardware must be protected from unauthorised access. All computer rooms are kept locked. Only authorised persons requiring regular access or access out of hours are issued with keys.

The following procedures must be adhered to at all times:

- Only IT Technical Support staff shall have access to the Computer Rooms.
- Only IT Technical Support staff may admit visitors to the Computer Rooms.
- Visitors are not permitted to connect any electrical equipment within the computer room without the express permission of the IT Technical Support Team
- Visitors to the computer room are not required to sign in but must be accompanied at all times.

Policy Area: Portable Computers

Policy Objective

To protect against damage or loss of either portable equipment or data.

Note

You are responsible for the portable computer and the data it contains whilst it is in your care.

Do

- Store portable computers securely when not in use.
- Ensure that portable computers have been marked with security tags and details have been entered into the organisation's hardware inventory.
- Ensure that anti-virus software is installed and up to date.
- Ensure files containing personal or confidential data are adequately protected and are not left on the computer on return.
- Be responsible for the backup of data stored on the portable computer.

Don't

- Leave portable computers where they can be easily stolen.
- Install unlicensed or unauthorised software on portable computers.

Policy Area: Organisation Servers

Policy Objective

To protect the integrity of the hardware and data stored on organisation file servers.

Note

The continued operation of the organisation IT system and the support for vital organisation business processes are dependent on the continued operation of the servers.

Do

- Ensure that the Technical Standards document is kept up to date and the information is accurate.
- Ensure that the servers are kept in a secure environment that limits the possibility of unauthorised access.
- Maintain suitable environmental conditions which will not jeopardise the effective running of the servers.
- Operate the planned backup procedure so that in the event of a loss of a server the data can be restored without adversely affecting the operation of key organisation systems.
- Store backup tapes off-site in a secure fireproof safe.

Don't

- Allow any unauthorised access to the server rooms.
- Install unauthorised or unlicensed software on servers.
- Give unrestricted access to the servers to third party suppliers for the purposes of support and/or maintenance.

Policy Area: Virus Protection

Policy Objective

To protect against software attacks by ensuring anti-virus software is installed, used, and updated at an appropriate frequency.

Note

The deliberate introduction of any virus or any other such software to organisation computers is a serious matter. Users are required to respond to any "virus warning" that may be displayed on the computer by immediately contacting a member of the IT Technical Support team. Continued use of the computer in these circumstances is expressly forbidden.

Do

- Ensure that anti-virus software is being used.
- Ensure that virus-checking software is updated on a regular basis.
- Ensure that floppy disks and other removable media are virus checked before use on the organisation network.
- Contact immediately the IT Technical Support team on the discovery of a virus.

Don’t

- Download unauthorised files or software from the Internet.
- Open email messages that contain suspicious attachments or come from an unknown source. Contact the IT Technical Support team for advice if you receive such an email.
- Install unlicensed or unauthorised software on organisation equipment.
- Use unauthorised screensavers.
- Continue to use a computer after a virus alert.

Policy Area: Backup and Maintenance of Data

Policy Objective

To ensure key data can be recovered following accidental or deliberate damage to the original copy of the data.

Note

Network storage space is limited. Users are required to manage their use of disk storage facilities on the organisation IT systems. The organisation will ensure that data held in the user areas will be backed up in accordance with the organisation policy.

Do

- Clear out / delete old files to save disk space.
- Remember that a student's network storage area will be maintained for one year after they leave organisation, after this point it will be deleted.
- Dispose of sensitive printouts by shredding.

Don't

- Delete, modify, or remove files from the computer where such files were not created by you.
- Change system settings without proper authorisation.
- Leave removable storage media or printouts in unsecured areas.

Policy Area: E-Mail

Policy Objective

To ensure the effective and appropriate use of e-mail facilities.

Note

The email system is the property of the organisation. All data and other electronic messages within this system are the property of the organisation.

The organisation reserves the right to monitor access and disclose the contents of all e-mail messages composed or received on the email system in accordance with its legal and audit obligations, and for legitimate operational purposes.

The e-mail system is not a secure means of communication. It is your responsibility to ensure it is used appropriately.

To prevent unwanted e-mail (spam) being delivered to user accounts, the organisation will use a filtering system to quarantine suspected e-mails.

Do

- Delete mail once it has been dealt with in order to conserve disk storage space. The organisation E-mail and facilities are not intended to act as filing systems.

Don't

- Send offensive, abusive, sexist, or anonymous messages.
- Send unsolicited or indiscriminate e-mail to groups of users.
- Use email for any form of harassment whether through content, language, frequency, or size of message.
- Create or forward 'chain letters', or other 'pyramid' schemes of any type.
- Subscribe to user/news groups or mailing lists on the Internet that result in large quantities of Internet traffic. The organisation reserves the right to block e-mail on entry in these circumstances.

Policy Area: Internet Access

Policy Objective

To provide individual, authorised access to the Internet and associated services, including access to BT EFM.

Note

The Internet provides access to a variety of information some of which may be deemed inappropriate if accessed in organisation. It is your responsibility to ensure it is used appropriately.

The organisation will use monitoring and filtering software to prevent access to the sites which may have an illegal or inappropriate content. User attempts to access these and other sites will be monitored and recorded. The organisation will undertake periodic reviews of the access logs to ensure appropriate use.

Do

- Virus scan all downloaded files prior to being opened or executed.
- Logoff when you have finished or are away from your desk.

Don't

- Access the Internet from an account other than your own.
- Download unauthorised or unlicensed software.
- Access, view or download information, graphics, pictures etc. that are deemed to be defamatory, obscene, racist, sexist, or may be of a criminal nature.
- Use the Internet to set up or run a personal business or for financial gain.
- Infringe copyright by downloading, copying, or distributing copyright protected material from the internet.

Policy Area: Remote Access (including data/files stored on removable media)

Policy Objective

To provide guidance on working securely from outside of the organisation network.

Note

The organisation provides access to various systems from outside of the organisation network. These include but are not limited to:

- E-mail
- Website
- Leaner portal
- Remote VPN Access

While precautions are taken to ensure the safeguarding of sensitive organisation data within the organisation network it is the remote user that should take responsibility for the security and safeguarding of data outside of this environment.

Do

- Only download or access data/files that you need to.
- If other users have access to the machine you are using, secure any organisation data/files in a password protected area.
- Secure any removable media with passwords.
- Ensure that you log off from any organisation services when leaving your computer.
- Keep your passwords secure.

Don't

- Download or distribute any data/files from the organisation provided services.
- Leave organisation data/files in publicly accessible areas on shared computers.
- Leave removable media in a non-secure location.
- Leave removable media without any password protection.
- Leave a computer unattended while logged in to organisation services.
- Distribute your passwords to any other person.

Reporting Incidents

The organisation will investigate all security incidents. It is the responsibility of staff and students to report any such incidents in accordance with the information in this policy.

A security breach is:

- Any action that results in or could result in the loss or damage to organisation assets and data.
- The unauthorised access to or disclosure of data and information.
- Any lapse in security.

Responsibilities

Security incidents will be reported to the CHISONA ACADEMY Data Protection Controller who will undertake an initial investigation, log the incident and report to the relevant Director. The organisation SLT will then gauge the scale of the incident and decide on further action.

Monitoring and Evaluation

Policy will be reviewed in light of every reported incident. Each year the log of security incidents will be investigated to determine the effectiveness of the Information Security Policy.

This review will take place between the Head and Management Team and any changes to the Information Security Policy will be directed to the change control procedure.

Sanctions

Breaches of this policy by staff, students or user authorised to access CHISONA ACADEMY systems will be dealt with under the appropriate disciplinary procedures. This may lead to the user's access to the IT System being suspended or restricted.

Breaches of this policy by staff will be dealt with under the appropriate disciplinary procedures.

Where an offence is committed under a criminal law, it will immediately be reported to the Police.

In the event of loss being incurred by the organisation as a result of a breach of these regulations by a user, that user may be held responsible for reimbursement of that loss.

Relevant Legislation

Where applicable, use of the IT facilities is subject to the provisions of (amongst others):

Freedom of Information Act 2000
Regulation of Investigatory Powers Act 2000
Data Protection Act 1998
Copyright, Design & Patents Act 1988
Computer Misuse Act 1990
Equality Act 2010
Counter Terrorism and Security Act 2015

These are examples of relevant legislation and not an exhaustive list of all the legislation that the organisation is bound by now or in the future.

More Information

Further information and guidance can be obtained from the following.

CHISONA ACADEMY ICT Team
Management Team
Director

Related Policy Areas and Guidelines

The following policies and guidelines support this policy:

- CHISONA ACADEMY GDPR Policy
- CHISONA ACADEMY Staff Handbook
- CHISONA ACADMEMY Child Protection and Safeguarding Policy
- CHISONA ACADEMY Health and Safety Policy