

## IT Policy

### Policy Statement

Staff and learners will have access to the internet for research and education purposes, and Welcome Skills welcomes this as a means for improving the IT skills of users and for enhancing the teaching and learning process..

### Requirements for Implementation

#### Rules

1. Users must not attempt to access or upload on the Internet, information that is obscene, sexually explicit, racist, defamatory, incites or depicts violence, or describes techniques for criminal or terrorist acts.
2. Users must not intentionally access or transmit computer viruses, or attempt to 'hack' into data that may damage the network.
3. Users must not infringe copyright - this includes unauthorised downloading of software from the Internet, including games, music files - MP3 files, and commercial screensavers.
4. Users must not knowingly undertake any action that will bring the company into disrepute.
5. Information sent by email may become subject to the Data Protection Act, and this must be complied with where appropriate.
6. Email must not be used for unsolicited advertising.
7. Persons sending email must not flood the network by sending unnecessary information to all users. This uses bandwidth on the network, and server space, and may prevent important information getting through. This is particularly important when sending attachment files and documents.

Any breach of these rules will result in disciplinary action.

This absence policy will be reviewed annually by the Board of Directors and amended as is necessary and any such changes will be communicated to all learners and staff.

### IT Code of Conduct

This code of conduct should be read in line with the Internet Policy, Data Protection policy and the Data Protection Act 1988.

DOCUMENT NAME/LOCATION	Date Produced	Version Number	Authorised By:	Document review date
IT Code of Conduct	July 2021	6	K.Hussin	June 2022

## Information Security

Under no circumstances should you gain access or attempt to gain access to information stored electronically which is beyond the scope of your authorised access level.

## Computer Software

- To avoid potential virus infection and consequent damage to the organisation, you must not load any software onto any computer without prior management approval. Approval will only be given after virus checking.
- Virus protection software is maintained and periodically updated.
- Under no circumstances must you load games or free issue software onto the organisation's equipment.
- If a specific application programme is necessary for your work, then it will be purchased by the organisation for your use.
- You must not make 'pirate' copies of organisation owned software for use by other persons either inside or outside the organisation. This not only breaks organisation rules, it is an illegal practice.
- Failure to comply with any procedure will give rise to disciplinary action taken against you, and this includes dismissal.

## Electronic mail policy

- The use of Welcome Skills' computer system is provided for business purposes only. A small amount of personal use is permitted as long as it is not excessive and does not interfere with the normal business activity of the organisation.
- The company reserves the right to access employee's mailboxes to assist with technical problems or to investigate breach of this policy.
- Internet email is not a secure medium of communication. It can be intercepted and read. Do not use it to communicate anything you would not wish to be made public.
- Never expect any email messages you receive to be completely private.
- Emails might be seen during the course of maintenance work on the network particularly by authorised third parties.

DOCUMENT NAME/LOCATION	Date Produced	Version Number	Authorised By:	Document review date
IT Code of Conduct	July 2021	6	K.Hussin	June 2022



- Do not forward email messages unless the originator of the message is aware the message may be forwarded.
- Do not sign onto email and leave your desk for long periods of time without logging off as it allows other employees direct access to your email.
- Always remember to disconnect from 'dial up' services once you have finished using Internet Explorer.

**Staff are forbidden using electronic mail for:**

Private business activities

- The receiving, sending or downloading abusive materials or offensive material to individuals or organisations.
- Sending chain letters
- Creating or forwarding email that contains abusive language. This includes racial or sexual discriminatory words and phrases.

**To ensure that this policy is adhered to, the content of your email can, and will be monitored by Directors.**

DOCUMENT NAME/LOCATION	Date Produced	Version Number	Authorised By:	Document review date
IT Code of Conduct	July 2021	6	K.Hussin	June 2022