Online Acceptable Use Policy

Pathway CTM Limited

Office: 0208 059 0710

VAT No: 262 6034 22

Company No: 09545140

www.pathwayctm.com

Contents

This Acceptable Usage Policy covers the security and use of all our information and IT equipment. It also includes the use of email, internet, voice, mobile IT equipment and appropriate contact with children, young people and adults at risk. This policy applies to all staff, contractors and agents (hereafter referred to as 'individuals'). This policy applies to Pathway CTM also referred 'the company' or 'we'.

This policy applies to all information, in whatever form, relating to all (Pathway CTM's) business activities, and to all information handled by the company relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Pathway CTM or on its behalf.

Computer Access Control – Individual's Responsibility
Access to our IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on our IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any company IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access the IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Pathway CTM's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Pathway CTM authorised device to our network or IT systems.
- Store Pathway CTM data on any non-authorised equipment.
- Give or transfer Pathway CTM data or software to any person or organisation. outside the company without the authority of the CEO.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use
Use of Pathway CTM internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the company in any way, not in breach of any term and condition of employment and does not place the individual or Pathway CTM in breach of statutory or other legal obligations.

All staff have a responsibility to keep students safe and to protect them from abuse (sexual, physical and emotional), and neglect and contextual safeguarding concerns. Staff should be aware that they are accountable for their actions on the internet and email systems, the way in which they exercise authority, manage risk, use resources and safeguard students. They must be aware of systems within the company which support safeguarding, which will be explained to them in the Staff Safeguarding Handbook, as part of staff induction and in regular staff training sessions.

It follows that trusted adults are expected to take reasonable steps to ensure their safety and well-being. Failure to do so may be regarded as professional misconduct. Whilst every attempt has been made to cover a wide range of situations, it is recognised that any guidance cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the guidance given by the company. It is expected that in these circumstances staff will always advise their senior colleagues of the justification for any such action already taken or proposed.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Pathway CTM considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Pathway CTM, alter any information about it, or express any opinion about the company, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Pathway CTM mail to personal (non-Pathway CTM) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of the company unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download any software from the internet without prior approval of your line manager.
- Connect Pathway CTM devices to the internet using non-standard connections.
- Contravene guidance as laid out in Pathway CTM's suite of safeguarding policies.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, we enforce a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with company remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Pathway CTM authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software
Individuals must use only software that is authorised by Pathway CTM on Pathway CTM computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on company computers must be approved by the Pathway CTM.

Individuals must not

- Store personal files such as music, video, photographs or games on company IT equipment.

Viruses
Pathway CTM has implemented centralised, automated virus detection and virus software updates within the company. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved company anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use
Use of Pathway CTM voice equipment is intended for business use. Individuals must not use company voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use Pathway CTM voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators unless it is for business use.

Actions upon Termination of Contract
All Pathway CTM equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the company at termination of contract.

All Pathway CTM data or intellectual property developed or gained during the period of employment remains the property of Pathway CTM and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering
All data that is created and stored on company computers is the property of Pathway CTM and there is no official provision for individual data privacy, however wherever possible the company will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Pathway CTM has the right (under certain conditions) to monitor activity on its systems, including internet, mobile phone and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018 the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

Online Contact with Children, Young People and Adults at Risk
Individuals must agree to adhere to the guidelines as laid out in Pathway CTM's safeguarding suite of policies including Safeguarding Policy and Staff Safeguarding Handbook. Iindividuals should not request or respond to any personal information from students other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

Individuals should not give their personal contact details to students for example, e-mail address, home or mobile telephone numbers, details of web-based identities. If a student locates these by any other means and attempt to contact or correspond with the individual, the adult should not respond and must report the matter to their line manager. The student should be firmly and politely informed that this is not acceptable. This must be reported to the DSL immediately.

It is the individual's responsibility to raise any issues of suitability (dress, setting, behaviour, communication) with the student immediately and end the online interaction if necessary. If staff believe that a student is recording the interaction, the lesson should be brought to an end or that student should be logged out immediately. If staff need to contact a student or parent by phone and do not have access to work phones, they should discuss this with the DSL and if there is no alternative always use 'caller withheld' to ensure their personal contact details cannot be identified.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 2018
- Guidance for Safer Working Practice for Those Working with Children & Young People in Education 2019

It is your responsibility to report suspected breaches of security policy without delay to your line manager or CEO.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Pathway CTM's disciplinary procedures.

Chris McNamara (Jan 20, 2021 21:14 GMT)

Chris McNamara
CEO

DOCUMENT CONTROL	
Doc Ref:	December 2020
Document Full Title	Online Acceptable Use Policy
Document Version number	V.2
Document stored in	Safeguarding Support Limited
Owned by:	Pathway CTM
Authorised by:	Chris McNamara
Date:	December 2020
Review Date:	December 2021
Circulation:	All Staff and Volunteers Website Clients