ICT Acceptable Use Policy

PETA Limited is committed to protecting employees, learners, training delivery partners and stakeholders from illegal or damaging action by individuals, either knowingly or unknowingly.

As a user of IT services of PETA Limited you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse the computing facilities in a way that constitutes a breach or disregard of the following policy you may also be in breach of other Company policies.

Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Learners, staff and training delivery partners who use their own devices to access the Company's online services are particularly reminded that such use requires compliance to this policy.

Learners and staff are directed to this policy during their induction and are required to acknowledge their agreed adherence to and compliance with the policy each time they log on to the network.

Purpose

The purpose of this policy is to outline the acceptable and unacceptable use of computer equipment or on-line services owned by PETA Limited, and acceptable or unacceptable general behaviour in areas of the Company where there is ICT equipment.

These rules are in place to protect PETA Limited employees and learners. Inappropriate use exposes PETA Limited and its stakeholders to risks including virus attacks, compromise of network systems and services, and legal issues.

The management of information security and the use of computers at PETA Ltd are framed by UK legislation including:

- Data Protection Act (2018)
- Counter-Terrorism and Security Act 2015
- Regulation of Investigative Powers Act (2000)
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- Counter-Terrorism and Security Act (2015)
- The Protection of Freedoms Act 2012
- Safeguarding Vulnerable Groups Act 2006

Scope

This policy applies to any person using PETA equipment or IT services. This policy applies to all equipment that is owned or leased by PETA Limited and to all equipment connected to the Company's network. Use of PETA Limited ICT equipment and the PETA Limited network are limited to staff, delegates, learners and authorised third parties only. Under no circumstances should any person not included in the above list be allowed to access the PETA Limited network.

Disciplinary Procedures

Staff or learners who contravene this policy may find themselves subject to the Company's disciplinary procedures. The ICT Systems Manager, as well as an individual's line manager or the Company Senior Management Team may take such disciplinary action.

Individuals may also be subject to criminal proceedings. The Company reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

Definitions

For the purposes of this policy the term **computing services** refers to any ICT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including wired and wireless access to the Internet).

The term **on-line services** includes services provisioned and accessible (both wired and wireless) through individual accounts and passwords. Such services would include access to internet/intranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP and are the property of PETA Limited. These systems are to be used for educational purposes in serving the interests of the organisation, and of our staff and learners in the course of normal operations.

The term **devices** includes but is not restricted to: computers, laptops, tablets and smart phones.

The term **ICT facilities** encompasses computing services, on-line services and devices as detailed above.

Key Principles

Authorisation and security

In order to use the ICT facilities of the Company a person must first be properly registered. Registration to use Company services implies, and is conditional upon acceptance of this Acceptable Use Policy as part of the Company regulations, for which a signature or electronic acknowledgement of acceptance is required. The lack of a signature does not exempt an individual from any obligation under this policy. The continuing use of the ICT facilities will be deemed to be acceptance by the user of the terms of this policy.

The registration procedure grants authorisation to use the core ICT facilities of the Company. Following registration, a username and password will be allocated to each individual user. Authorisation for other services may be requested by application to the ICT Systems Manager.

> **Any attempt to access, use or interfere with any user account or email address for which the user is not authorised, is prohibited and will be regarded as a disciplinary offence.**

No one may use, or attempt to use, ICT facilities allocated to another person, except when explicitly authorised.

Staff ICT Accounts have been allocated for use by the member of staff in connection with their job requirements. Learner ICT Accounts have been allocated for exclusive use by the learner in connection with their teaching, learning and assessment whilst at the Company.

A user must take all reasonable precautions to protect the Company's resources (including the ICT facilities and the Company's information and data), their username and passwords. Initial passwords should be reset on the first day.

The ICT Systems Department primarily responsible for securing PETA's systems and data, however all users must play their part by complying with the policies and respecting the security systems in place.

Unacceptable use may be summarised as, but not restricted to:

- Using the Company network for unauthenticated access;
- Attempting to access or actions intended to facilitate access to computer services, online services or devices for which the individual is not authorised;
- Sending emails that purport to come from an individual other than the person actually sending the message using, eg, a forged address;
- Attempting to break into or damage computer systems or data held thereon;
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, eg use of equipment which is inadequately protected against viruses and spyware;
- Interfering with data or settings in another person's network account;
- Connecting an unauthorised device to the Company network, ie one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy, and acceptable use;
- Circumvention of network access control;
- Monitoring or interception of network traffic, without permission;
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- Connecting any device to networks, including wireless, to which you are not authorised such as Wi-Fi provided in public places like coffee shops, restaurants and pubs, airports, hotels, shopping centres etc;
- Allowing third party access to the ICT facilities, either on site or remotely over the internet, without prior authorisation by the ICT Systems Manager.
- Allowing other people to use your account.
- Interfering with other users' work.
- Using software designed to unblock sites.

User conduct and purpose of Use

ICT facilities are provided primarily to facilitate a person's essential work as an employee or learner or other role within the Company. Use for other purposes, such as personal email or Internet use, is a privilege which can be withdrawn at any time and without notice. Any such use must not interfere with the user's duties or learning or any other person's use of computer systems and must not, in any way, bring the Company into disrepute.
Company email addresses and associated Company email systems must be used for all official Company business. All staff must regularly read their Company email and delete unwanted or unnecessary emails at regular intervals.

Users of PETA ICT facilities are expected to conduct themselves in a way which is mature, professional and compliant with relevant law.

Staff use of social networking sites during working hours (breaks excepted), other than for maintaining legitimate business contacts is not permitted. Please see the Social Media Policy for further information.

Commercial work (ie room hire) for outside bodies involving the use of the Company's ICT facilities which require a deviation from that which is provided as standard, requires explicit permission from the ICT Systems Manager and such use is liable to charge.

Unacceptable use may be summarised as, but not restricted to:

- Actions which cause physical damage to any ICT hardware, including peripherals (eg, mouse, cables, printers);
- Defamation;
- Unsolicited advertising, often referred to as spamming;
- Accessing, downloading, printing, copying, forwarding or otherwise transmitting any unlawful material, in the event of any use that could be regarded as giving rise to criminal proceedings the Company may inform the police or other law enforcement agency.
- Attempting to use the ICT facilities for the purposes of bribery;
- Unauthorised resale of Company services or information;
- Using the ICT facilities for gambling or gaming;
- Using the ICT facilities for carrying out any illegal trading activity.
- Conduct which may discredit or harm the Company, its staff or the ICT Facilities;
- Use of torrenting or peer-to-peer and related applications within the Company;
- Activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs, without permission;
- Excessive use of resources such as filestore, leading to a denial of service to others, especially when compounded by not responding to requests for action;

Copyright Compliance and data protection

Users may need to process certain information about its PETA's employees, volunteers, learners, customers, suppliers and other individuals they may come into contact with during the normal course of business. In so doing, all users must must comply with the General Data Protection Regulations (GDPR) and Data Protection Act 2018. More information can be found in the Data Protection Policy.

All users must also abide by laws relating to copyright and therefore must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose eg teaching or research then copyright permission must be obtained and documented before such material is used.

Employees and Learners are reminded that the Company treats plagiarism very seriously and will investigate any allegation ie the intentional use of other people's material without attribution.

PETA operates all software under appropriate licencing, so the use of pirated software is prohibited, please see the Software Policy for further information.

Unacceptable use may be summarised as, but not restricted to:

- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;

- Downloading, distributing, or storing music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- Distribution or storage by any means of pirated software;
- Unauthorised use or transmission of the company and/or client information;
- Downloading or installing illegal software onto a workstation.
- Downloading or copying any software from the Company network onto portable media, etc.
- Downloading, copying or removing from the system company and/or client information without permission
- Uploading your own personal software packages onto a Company workstation.
- Photographing or recording members of staff or Learners without their permission, using devices such as mobile phones, cameras or digital recorders.

Duty of care and safeguarding

PETA disapproves of all forms of anti-social behaviour, harassment, bullying or victimisation, and seeks to ensure that the working environment is sympathetic to all employees and learners. The Company recognises that it has a duty of care to its staff, learners, customers and stakeholders to deal with any anti-social behaviour, harassment, bullying or victimisation, which directly or indirectly relates to or affects a person's work, training or well being.

As a provider of education and training, and in accordance with legislation PETA has a moral and statutory duty to safeguard (including prevent) and promote the welfare of young people an vulnerable adults at its centres and this naturally extends to include the use of the ICT Facilities.

More detail can be found in PETA's Anti-social Behaviour and Harassment Policy and the Safeguarding and Prevent Policy.

Unacceptable use may be summarised as, but not restricted to:

- Sending offensive, abusive or inappropriate e-mails.
- Threatening, bullying, intimidating or harassing staff, learners or others;
- Accessing, creating, displaying, transmitting or downloading material that is fraudulent or otherwise unlawful, obscene, likely to cause offence or inappropriate including (but not limited to) Pornography, self-harm, drugs, violence;
- Accessing websites containing illegal content, such access may be subject to criminal proceedings.
- Accessing, creating, displaying, transmitting or downloading inappropriate or extremist materials, as defined within the Prevent Policy. PETA has a statutory duty to take steps to prevent individuals from being drawn into extremism and terrorism, and a duty to alert and to report any attempted access to, or dissemination of inappropriate material which is either created, accessed, transmitted or downloaded;

Privacy and Monitoring

All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person. Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

The Company reserves the right to monitor email, telephone and any other electronically mediated communications, whether stored or in transit, in line with relevant law.

Reasons for such monitoring include the need to:

- Prevent learners from becoming radicalised and/or from being drawn into terrorism or extremist violence
- Safeguard learners and identify if there is a suspicion that a learner may be at risk, under threat or a victim of any activities or actions which may cause harm to the learner.
- Establish the existence of facts (eg to provide evidence of commercial transactions in cases of disputes);
- Investigate or detect unauthorised use of the Company's telecommunications systems and ensure compliance with this policy or other Company policies;
- Ensure operational effectiveness of services (eg to detect viruses or other threats to the systems);
- Prevent a breach of the law or investigate a suspected breach of the law, the Company's policies and contracts;
- Monitor standards and ensure effective quality control.

In addition, the Company reserves the right for appropriately authorised staff to examine any data including personal data held on Company systems. Certain staff within the Company have been authorised to examine files, emails and data within individual accounts, but will only do so when operationally necessary.

It is also occasionally necessary to intercept network traffic. In such circumstances appropriately authorised persons will take all reasonable steps to ensure the privacy of service users.

When a learner or member of staff leaves the Company (either on completion of training or termination of employment) data held on any of the company's ICT facilities remains the property of the company. The Company is under no obligation to recover any data once a person has left the Company.

When a member of staff is away it may be necessary for appropriately authorised members of staff to access the absent member of staff's email account to deal with matters in their absence. This should be borne in mind when using the ICT facilities for personal reasons.

For operational reasons and for the continuing delivery of services, the Company has the right to access the network and email account of an individual after that person leaves.

Users of ICT facilities should be aware that the Company conducts random monitoring of communications, regardless of whether the use is business or personal.

Where abuse is suspected (especially criminal activity and/or gross misconduct), the Company may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the CEO or other appropriate senior person.

The Company is committed to achieving an environment which provides equality of opportunity, and freedom from discrimination. Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene Company codes on harassment. No carrying out of unauthorised surveillance, audio and/or visual, of a learner, staff or member of the public on PETA Limited premises is permitted.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

Users of services external to the Company are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. The use of Company credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

Responsibilities

1. This policy is the responsibility of the ICT Systems Manager.
2. The ICT Systems Manager is responsible for the installation and maintenance of all ICT facilities within PETA and the logging and monitoring of the security systems in place.
3. All Company Managers are responsible for the implementation and monitoring of the policy including copyright compliance monitoring of teaching and learning resources.
4. All users have a responsibility to comply with this policy.
5. The responsibility for the supervision of the Acceptable Use Policy is delegated to the ICT Systems Manager by the Company SMT. Any suspected breach of this policy should be reported to this person who in conjunction with a Senior Manager determine the appropriate action within the Company's disciplinary framework. The Company reserves the right to audit and/or suspend without notice any account pending any enquiry. Where necessary, this will include the right to intercept communications.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered here at present. In the first instance Learners should address questions concerning what is acceptable to their trainer assessor or mentor. Staff should approach their line manager.

Where there is any doubt the matter should be raised with ICT Systems Manager, who will ensure that all questions are dealt with at the appropriate level within the Company.

Summary

Please remember:

- ▲ Copyright regulations apply to electronic sources - please check before you make use of, print, copy or upload to Moodle or any other internet source.
- ▲ You must logout from or lock access when leaving a computer, even for a short time.
- ▲ You must be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc) has been electrically tested, before using it on PETA premises.
- ▲ Anyone found abusing the ICT Acceptable Use Policy may be subject to disciplinary action.

Company computers are provided primarily for Company work or purposes of education. However, you may use the equipment for personal use providing you do not breach the Acceptable use Policy.

If you use the Company equipment for personal use you should note the following:

- Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.
- This Acceptable Use Policy applies to both wired and wireless access and use of network on your own devices or on Company equipment.
- In order to use the ICT facilities of the Company a person must first be properly registered.
- Registration to use Company services implies and is conditional upon acceptance of this Acceptable Use Policy.
- The continuing use of the ICT facilities will constitute an acceptance of the terms of this policy by the user.