Bounce Animal Rescue - Acceptable Use Policy

November 21, 2019

This Acceptable Use Policy covers the security and use of all Bounce's information and IT (Information Technology) equipment. It also includes the use of email, Internet (including Social Media Platforms), voice, and mobile IT equipment. This policy applies to all Bounce's employees, contractors and agents (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to Bounce's business activities and to all information handled by Bounce relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by Bounce or on its behalf.

Computer Access Control – Individual's Responsibility

Access to the Bounce IT systems is controlled by use of User IDs, passwords, and other methods (hereafter referred to as 'access'). All access is to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on Bounce's systems.

Individuals must not:

- Allow anyone else to use their access on any Bounce system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Bounce's IT systems.
- Leave their password unprotected (e.g. writing it down).
- Perform any unauthorized changes to Bounce's IT systems or information.
- Attempt to access data that is not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-Bounce authorized device to the Bounce network or IT systems.
- Store Bounce data on any non-authorized Bounce equipment.
- Give or transfer Bounce data or software to any person or organization outside Bounce without the authority of Bounce.
- Ensure that individuals are given clear direction on the extent and limits of their authority regarding IT systems and data.

Internet and email Conditions of Use

Use of Bounce 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 Bounce in any way, not in breach of any term and condition of employment, and does not place the individual or Bounce in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the Internet and email systems.

Individuals must not:

- Place any information on the Internet and social media platforms that relate to Bounce, alter any information about Bounce, or express any opinion about Bounce, unless specifically authorized to do so.
- 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 Bounce 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 in relation to Bounce activities.
- Use the email systems in a way that could affect its reliability or effectiveness (e.g. distributing chain letters or spam).
- Send unprotected sensitive or confidential information externally.
- Forward Bounce mail to personal (non-Bounce) email account(s).
- Make official commitments through the Internet or email on behalf of Bounce unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files, etc. without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download any non-business software from the Internet without prior approval.
- Connect Bounce devices to the Internet using non-standard connections or appropriate security measures.

Clear Desk and Clear Screen Policy
In order to reduce the risk of unauthorized access or loss of information, Bounce enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided (e.g. secure print on printers).
- Computers must be logged off, locked, or protected with a screen locking mechanism controlled by a password of at least 6 characters when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All confidential 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:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops and confidential information must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise (e.g. at home or in public places).
- 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 (at least 8 characters) or a PIN (at least 6 characters) and, when 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 Bounce authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software
Employees must use software that is authorized by Bounce on Bounce’s computers. Authorized software must be used in accordance with the software supplier's licensing agreements.

Viruses
All devices must have antivirus and malware 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 using approved Bounce anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use
Use of Bounce voice equipment is intended for business use first and personal use second.
Individuals must not:

- 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 Bounce equipment and data including but not limited to laptops and mobile devices including telephones, smartphones, USB memory devices, and CDs/DVDs, must be returned to Bounce at termination of employment or contract. All Bounce data or intellectual property developed or gained during the period of employment remains the property of Bounce and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

- All data that is created and stored on Bounce computers is the property of Bounce and there is no official provision for individual data privacy.
- System logging may take place where appropriate and investigations will commence where reasonable suspicion exists of a breach of this or any other policy. Bounce has the right (under certain conditions) to monitor activity on its systems, including Internet 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 within any law or mandate from any government entity.

It is your responsibility to report suspected breaches of security policy without delay to your line management or the Board immediately. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Bounce's disciplinary procedures.