Keystone Acceptable Use Policy

Keystone Learning Services, ("Keystone") Acceptable Use Policy ("AUP") is intended for Keystone products and services with the goal of protecting Keystone Subsidiaries, Affiliates, Employees, and Customers. This policy applies to the use of all Keystone products, websites, copyrights, and services owned or operated by Keystone, as well as any and all data sent, transferred, received, stored, or accessed in the Keystone network. Other products or services offered by Keystone may have additional terms and conditions that govern over this policy in the case of inconsistencies.

This AUP and the following prohibited activities below is an integral part of your hosting agreements with Keystone. Keystone services are for the lawful use of Keystone Customers and if Keystone finds you in violation of the below prohibited activities your services may be subject to suspension and/or removal from Keystone network. This policy is a non-exclusive list of actions prohibited by Keystone. Keystone reserves the right to modify these policies at anytime, changes become effective immediately upon posting of this page

SECURITY

Keystone assumes no legal liability for the actions or data created, or posted by its Customers. Each Customer is responsible for all data transmitted, or received by, to, or through Keystone services. Keystone will cooperate with law enforcement on any criminal or suspected criminal acts by means which Keystone may deem necessary including but not limited to handing over personal information, data, or hardware to aid law enforcement with their investigations. Law officials may request that you not be notified on issues relating to criminal acts; Keystone reserves the right to comply with this request.

PURPOSE

This Acceptable Use Policy has been formulated with the following goals in mind:

- Ensure the security, reliability and privacy of Keystone's network and systems, and the networks and systems of others.
- Preserve the value of the Internet as a resource for information and free expression.
- Preserve the privacy and security of Keystone Customers and other Internet users.
- Discourage irresponsible practices which degrade the usability of network resources and thus the value of Internet services.
- Avoid situations that may cause Keystone to incur legal liability.
- Maintain the image and reputation of Keystone as a responsible provider.

Keystone operates under a strict "No Spam" policy. The sending of any unsolicited e-mail advertising messages from, to, or through Keystone's services may result in the imposition of civil liability against the sender, in accordance with California Business & Professions Code Section 17538.45. A copy of the California Business & Professions Code may be obtained on-line from http://www.leginfo.ca.gov. Keystone reserves the right to check all known commercial and public databases for information regarding prior history of unsolicited mail sending, and blacklisting, and may choose to deny or terminate services based on this information. Individuals identified as "ROKSO" level abusers will be denied service immediately. Keystone uses the databases of associations such as Five-Ten Software Group, MAPS, SORBS, Spamhaus, UCE protect, Njabl, and CBL to identify previous and current spammers. Keystone receives feedback from other large ISPs about spam their Customers report, ISPs such as Road Runner, Comcast, SBCglobal, MSN, and Outblaze.

1. SPAM

To protect outside sources Keystone's Solicited Bulk E-mailers they are required to remove complaints by methods including but not limited to creating a no-mail list. Keystone respects the CAN SPAM act; however, you as a Customer are required to follow a stricter Double Opt-In policy as well as having an opt-out in all e-mails. Bulk e-mailers may be required to provide the complete opt-in information as well as provide proof of previous business relationships with the recipients.

You may not make Usenet postings which advertise a website, e-mail account, or other service provided by or through Keystone, to any newsgroup whose charter does not specifically allow such advertisements. You may not send unsolicited bulk e-mail (UBE) or post advertisements to Usenet (except where specifically allowed by newsgroup charters) from a service provided by or through Keystone. You may not host "spam-friendly" Web sites, including spam software sites. You may not send UBE which advertises a website, e-mail account, or other service provided by or through Keystone. You may not send e-mail to any person who does not wish to receive it. If a recipient asks to stop receiving email, the Customer must immediately and permanently cease to send that individual any further e-mail.

1. **E-Mail Spam/Unsolicited Bulk E-Mail(UBE)/Unsolicited Commercial E-mail(UCE)** — Use of services to send e-mails to users in a pre-generated list or self created list. Unsolicited Bulk / Commercial E-mails are sent to users that do not wish to receive the e-mail notification of products you wish to sell or advertise.
    1. *Mobile Phone Spam* — Use of e-mail services to send unsolicited text messages advertising a product or website.
    2. *Forum Spam* — Use of e-mail services to advertise or post on a forum content related to a product you wish to sell.
    3. *Newsgroup Spam* — Use of e-mail services to advertise or commit forgery through the use of newsgroups
    4. *Blank Spam* — Use of e-mail services to E-mails containing no subject or content. Commonly used as a harvesting tactic designed to find valid e-mail addresses.
2. **E-mail Address Harvesting** — Use of Keystone services to obtain or create unconfirmed mailing lists with the intention of selling, distributing, or spamming is strictly forbidden.
    1. *Spam Bots* — A script or program that searches human readable text for e-mail addresses and collects them in an e-mail list.
    2. *E-mail List Gathering Programs* — Other scripts or programs that are used for gathering e-mail address from varying sources.
3. **Spamvertising** — Sending spam with content advertising websites, or containing IPs that are on Keystone services, or sending spam from Keystone services advertising web content outside of Keystone networks is prohibited.

2. HARMFUL MATERIALS

Use and access to Keystone services is for lawful use only, and it is the responsibility of the Customer to use their best judgment of what is acceptable material. Using Keystone's network, services, or systems to store or send content which is illegal according to the laws of United States of America, the state of New York, the city of Albany, or any International treaties respected by the United States of America, is not permitted for any reason. You may not display, transmit, advertise, distribute, or sell harmful materials. You may not store or send any material deemed either illegal or inappropriate from Keystone networks, including but not limited to child pornography.

1. **Material Harmful to Minors** — Images depicting persons under the age of 18 engaging in unlawful sexual acts, Pornographic materials viewable by persons under the age of 18 without proof of age.

2. **Obscene Content** — E-mails, messages, phone messages, or posts with content that is threatening, or harassing any other individual. Harassment, whether through content, frequency, or size using e-mail or Usenet messages.
3. **Destructive Programs** — Software or hardware containing programs such as Viruses, Worms, Trojans or other malicious programs with intent of causing harm to an individual's computer or server.

3. COPYRIGHTED MATERIALS

Keystone expressly forbids the use of copyrighted materials without written permission from the owner of that material. Keystone follows all rules and regulations set forth by the DMCA ("http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:"). You may not engage in an attempt to infringe, store or send any material deemed either illegal or inappropriate for Keystone networks, including but not limited copyrighted images, software, or music.

1. **Copyright Infringement** — Advertising, selling, distributing, or marketing material that infringes a copyright, trademark, or any other proprietary right to any intellectual property including but not limited to photographs, trade secrets, and/or property.

4. FRAUDULENT MATERIALS

Keystone requires that all Customers provide accurate information regarding name, address, and a working phone number to identify each Customer. You may not use Keystone services to impersonate another individual by altering source IP address information, or forging e-mail/Usenet headers or other identifying information. You may not make any attempt to fraudulently conceal, forge, or otherwise falsify one's identity in connection with use of the Keystone service. Customers must not utilize Keystone services to distribute fraudulent materials to others.

1. **Fraudulent Activities**
    1. Attempting to buy or sell products or services, or offering fraudulent goods, services, or promotions.
    2. Forwarding or otherwise propagating chain letters or "e-mail hoaxes," whether or not the recipient wishes to receive them, unless such propagation is both solicited and in the clear context of debunking or discrediting chain letters/hoaxes.
2. **Forgery or Disguising Your Identity**
    1. Falsifying or modifying data to fraudulently disguise you as someone else with the intention of deceiving another user, including but not limited to forging e-mail Headers or e-mail "munging".
    2. Transmitting any electronic communication, including e-mail, using the name or address of another person or organization, for purposes of deception.
    3. Impersonating another individual by altering source IP address information, or forging e-mail/Usenet headers or other identifying information.

5. PHISHING MATERIALS

The use of Keystone services to gather personal information about victims of phishing is strictly forbidden. You may not perpetrate, engage in, or take part in the use of phishing scams. Including but not limited to Impersonating another individual by altering source IP address information, or forging e-mail/Usenet headers or other identifying information.

1. **Phishing Scams** — Including but not limited to sending e-mails with links to bogus websites that look similar to actual sites, or sending e-mails about you impersonating a representative of Paypal, Ebay, or

Bank Employee, with the intention of acquiring personal information such as credit card information, Social Security Number, personal e-mails, home addresses, etc.

6. HACKING

Use of Keystone services to perform attacks on other servers or computers, outside of, or within Keystone premises is strictly forbidden. You may not Intercept or attempt to intercept, through any method, network traffic intended for other Customers. You may not use or store any type of software which is designed to, or is likely to, abuse or negatively impact internet service, including, but not limited to, port scanners, hacking tools, ping flooding programs, security/root exploits, packet sniffers, and spam software. Denial of service, including, but not limited to, any form of Internet packet flooding, packet corruption, or abusive attack intended to impact the proper functioning of any party's internet servers or services are forbidden.

1. **Hacking** — Use of the service to breach or access a person's server, computer, or software with the intent of gaining access to or destruction of data without that person's permission or consent.
2. **Net Scanning** — Use of services to search outside networks for open firewalls, or server ports in an attempt to exploit a vulnerability or weakness in the device.
3. **SSH attacks / Brute Force attack / Dictionary Attack** — Using the services to engage in an attack on a separate entities server or computer with an unlawful script or program that attempts to guess a users credentials.
4. **DDos/Dos Attacks** — An attack on a person's network, server, or computer that creates multiple requests repetitively in an attempt to slow down or crash that person's network connectivity
5. **Ping/Syn Floods** — An attack that creates multiple echo requests and sends them to its target repeatedly in an attempt to slow down or crash the targets network connectivity.

7. PROXY

Keystone services do not allow others to openly relay e-mail or services through your servers. You may not allow the use of another party's electronic mail server to relay e-mail without express permission from Keystone. Running proxy servers, such as squid or BNC, unless they are available only to users whose verified contact information is known by the proxy operator and can be disclosed to Keystone or law enforcement authorities upon request. All usage of such services must be brought to the attention of the Keystone security team and cleared by the Security Manager before you begin running such services.

1. **Mail Proxy** — Use of Keystone services to run any kind of Mail Proxy is not permitted.
    1. *Open Mail Proxy* — A server that has been set up to allow any user to relay mail through it.
    2. *Secure Mail Proxy* — A server that has been set up to only allow specific users to relay their mail through it.
2. **Web Proxy** — A server that allows users to forward requests to other servers. Keystone may allow certain proxy servers at their own discretion and under separate terms.
    1. *Open Web Proxy* — A proxy server that allows users to remain anonymous.

ENFORCEMENTS

Complaints about Customers/representatives or end-users of a Keystone Customer will be forwarded to the Keystone Abuse Department for action. If violations of the Keystone Acceptable Use Policy occur, Keystone reserves the right to terminate services or take action to stop the offending Customer from violating Keystone's AUP as Keystone deems appropriate, without notice. Violation of any Keystone AUP policies may be subject to a fine of up to $500 USD for each incidence of violation. Failure to respond or handle an issue of violation in a timely manner is considered a violation of this AUP.

CUSTOMER RESPONSIBILITIES

It is the responsibility of the Customer to ensure that all of their Customers abide by this policy. If a Customer wishes to use a dedicated server to send mail, it is the responsibility of the Customer to make sure that their Forward and Reverse DNS records match, to set a PTR record in the iBizPanel to a non-generic name, and if the Customer has a control panel on their server they must set a distinct non-generic PTR for each domain they plan to send mail from.