Acceptable Use Policy

This Acceptable Use Policy ("AUP") specifies the rules applicable and the actions prohibited to users ("Users") of the network and systems ("Systems") of UVU Africa NPC Group which for the purposes of this AUP shall be deemed to mean and include UVU Africa NPC (registration number 1999/002647/08), Bandwidth Barn (Pty) Ltd (registration number 2000/015304/07), Injini EdTech Acceleration NPC (registration number2017/193849/08), UVU Bio NPC (registration number 2019/075897/08) and any company falling within the same "group" of companies as UVU Africa NPC provided for in section 1 of the Companies Act 71 of 2008 ("UVU Africa NPC Group").

Please read this AUP carefully before using the Systems operated by UVU Africa NPC Group as Users are required to adhere to this policy in its entirety.

1. APPLICABLE LAWS AND REGULATIONS

1.1. UVU Africa NPC Group's Systems may be used only for lawful purposes and Users may not act in contravention of any applicable laws or regulations of the Republic of South Africa. Should the User reside outside of the Republic of South Africa, the laws of the country in which the User resides shall apply.

1.2. Any transmission, distribution, or storage of any material on or through the Systems in contravention of any applicable law or regulation is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secrets or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

1.3. The terms of this AUP are not to be construed as being exhaustive. On the whole, any conduct that violates any law, regulation, or the accepted norms of the Internet community, whether or not expressly mentioned in this AUP, is prohibited.

2. LIMITATIONS ON THE USE OF THE SYSTEMS

2.1. The User acknowledges that UVU Africa NPC Group is unable to exercise control over the content of the information passed over the Systems and the Internet and UVU Africa NPC Group is therefore not responsible for the content of any messages or other information transmitted over its Systems.

2.2. The User is not permitted to use its Internet access to disseminate any copyrighted materials, provided permission for such dissemination is granted to the User by the owner of the materials. The User may however obtain and download any materials marked as available for download off the Internet.

2.3. The User is prohibited from obtaining and/or distributing any unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, sexually explicit, profane, or hateful, or racially, ethnically, or otherwise objectionable content of any kind.

3. BREACH OF SYSTEMS AND NETWORK SECURITY

3.1. All references to systems and networks under this section includes the Internet (and all those systems and/or networks to which User is granted access through UVU Africa NPC Group and includes but is not limited to the Systems of UVU Africa NPC Group itself).

3.2. The User may not circumvent User authentication or security of any host, network, or account nor interfere with service to any User, host, or network.

3.3. Any User who commits any offence detailed in either the Electronic Communications and Transactions Act 25 of 2002 or the Cybercrimes Act 19 of 2020 shall, notwithstanding criminal prosecution, be liable for all resulting liability, loss or damages suffered and/or incurred by UVU Africa and its affiliates, agents and/or partners. UVU Africa NPC Group will investigate incidents involving such offences and will involve and co-operate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

3.3.1. unauthorised access to or use of data, systems, or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorisation of UVU Africa NPC Group;

3.3.2. unauthorised monitoring of data or traffic on the network or systems without express authorisation of UVU Africa NPC Group; and

3.3.3. interfering with, disrupting, or compromising access to or beneficial use of the Systems service by any other User.

3.4. The maintenance of the confidentiality of a User's password remains the sole responsibility of the User. In the event of a breach of security through a User's account, such User will be liable for any unauthorized use of UVU Africa NPC Group Systems, including any damages which result therefrom, until such time that the User informs UVU Africa NPC Group of such breach.

3.5. UVU Africa NPC Group shall, in its reasonable discretion, reserve the right to determine what constitutes a violation of this AUP.

4. FAIR ACCESS AND USE OF THE SYSTEMS

4.1. To ensure that all Users have fair and equal use of the service and to protect the integrity of the network, UVU Africa NPC Group reserves the right, and will take the necessary actions, to prevent improper or excessive usage thereof, including, but not limited to:

4.1.1. limiting throughput;

4.1.2. preventing or limiting service through specific ports or communication protocols; and/or

4.1.3. complete termination of service to Users who grossly abuse the network through improper or excessive usage.

4.2. This policy applies to and will be enforced for intended and unintended prohibited usage, such as viruses, worms, malicious code, or otherwise unknown causes.

4.3. Online activity will be subject to the available bandwidth, data storage and other limitations of the service provided, which UVU Africa NPC Group may, from time to time, revise at its own discretion and without prior notice to the User.

5. PROHIBITED ELECTONIC MAIL CONDUCT

5.1. The following activities are expressly prohibited:

5.1.1. sending unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements, etc.);

5.1.2. forwarding or propagating chain letters or malicious e-mail;

5.1.3. sending multiple unsolicited electronic mail messages or "mail-bombing" one or more recipients;

5.1.4. sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender; or

5.1.5. using redirect links in unsolicited commercial e-mail to advertise a website or service.

6. REPORTING UNACCEPTABLE USE

6.1. Upon receipt of a complaint, or having become aware of an incident, UVU Africa NPC Group reserves the right to:

6.1.1. inform the User's network administrator of the complaint or incident and require the network administrator to handle the incident according to the terms of this AUP;

6.1.2. in the case of individual Users, suspend the User's account and withdraw the User's network access completely; and

6.1.3. fine the offending parties for administrative costs as well as for resources lost due to the incident;

6.1.4. suspend access of the User to the network until the relevant unacceptable use can be rectified by appropriate means; and

6.1.5. share information concerning the incident with other Internet access providers, or publish the information, and/or make the Users' details available to law enforcement agencies.

6.2. Any one or more of the steps listed above, insofar as they are deemed necessary by UVU Africa NPC Group in its absolute and sole discretion, may be taken by UVU Africa NPC Group against the offending party. All cases of violation of the above Acceptable Use Policy should be reported to reception@uvuafrica.com.