COURTEVILLE BUSINESS SOLUTIONS PLC
...enabling systems

EXTRACT OF COURTEVILLE'S INFORMATION ASSET ACCEPTABLE USE POLICY :

PURPOSE : Policy is designed to establish acceptable and unacceptable use of electronic devices and network resources at Courteville Business Solutions Plc (hereafter referred to as 'the company', Courteville' or 'the organization').

SCOPE : All employees, contractors, consultants, temporary and other workers at Courteville, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned by Courteville, or to Mobile Devices that connect to Courteville's network or reside at the office.

DEFINITION(S):

Spam: means electronic junk mail, junk newsgroup postings or messages that are unsolicited, unwanted, and irrelevant.

Users: means all staff and third parties (including but not limited to contractors, independent agents, state official) operating on behalf of the Company or undertaking the Company's functions and thereby accessing the above systems or who are provided with a Company Issued Mobile Device

POLICY STATEMENT :

a. All employees, contractors, consultants, temporary and other workers at Courteville, including all personnel affiliated with third parties are responsible for exercising good judgment regarding appropriate use of Courteville resources in accordance with Courteville policies, standards, and guidelines. Courteville resources may not be used for any unlawful or prohibited purpose.

b. Users should be aware that the data they create on the practice systems remains the property of the company and Courteville reserves the right to audit networks and systems (including data/internet usage/email usage /etc.) on a periodic basis to ensure compliance with this policy.

c. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the Courteville's network may be disconnected.

Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

d. Users are responsible for the security of data, accounts, and systems under their control.

e. All Users are to keep their passwords secure and are not to share account or password information with anyone, including other personnel, family, or friends.

f. Users must ensure, through legal or technical means that proprietary information remains within the control of Courteville at all times. Conducting Courteville's business that results in the storage of proprietary information on personal or non-Courteville controlled environments, including devices maintained by a third party with whom Courteville does not have a contractual agreement, is prohibited. This specifically prohibits the use of an email account that is not allowed by Courteville or its customer and partners, for company business.

g. Users are responsible for ensuring the protection of assigned Courteville assets that includes the use of computer cable locks and other security devices. Laptops left in Courteville premises overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of Courteville assets.

h. All personal computers, laptops, and workstations must be secured with a password-protected screensaver as stated in the Company's Clear Desk and Clear Screen Policy.

I. Devices that connect to the Company's network must comply with the Access Control and Password Policy.

i. Users are responsible for the security and appropriate use of Courteville network resources under their control.

j. Users are strictly prohibited from the following;

1. Causing a security breach to either Courteville or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

2. Causing a disruption of service to either Courteville or other network resources, including, but not limited to, floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

4. Exporting or importing software, technical information, encryption software, or

technology in violation of international or regional export control laws.

5. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

6. Sending Spam via email, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

7. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

9. Use of the company's official email or IP address to engage in conduct that is illegal or violates Courteville's policies or guidelines.

10. Posting to a public newsgroup, bulletin board, or listserv with an official email or IP address represents Courteville to the public; therefore, Users must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

CONTACT AND COMMUNICATION: If you require further information or a copy of the policy, you may contact Legal or SCMU at our Head Office, 38, Commercial Avenue, Sabo, Yaba, Lagos.