IT POLICY

EMAIL USAGE POLICY

Email Usage Policy

All Operating Company staff are responsible for the content of emails which they send or forward from their corporate email account. Operating Company staff must ensure at all times that the content of any email is lawful and in accordance with the OCU Code of Business Conduct, particularly in relation to sexual harassment and offensive behaviour. All network and Instalcom email accounts may be monitored from time to time the company will inform all staff and personnel with such accounts of this fact.

Instalcom shall have the right to access all corporate accounts at any time in particular when unlawful conduct is suspected. Personnel should not use, store or forward corporate information on any personal email accounts. Instalcom reserves the right to inspect personal email accounts if it is suspected that corporate information is stored there. Instalcom will exercise its rights in this regard in accordance with Applicable Laws and the OCU Privacy Policy.

Operating Company staff should carefully consider the content of email messages as you would any other form of written correspondence; the effect in law of emailing is the same as sending a letter on Instalcom's headed paper. Remember that emails may have to be disclosed under certain privacy laws and as evidence in any court proceedings, litigation, arbitration, tribunals or investigations by regulatory bodies. Inappropriate content contained in emails may damage both your interests and those of Instalcom. Consider whether email is the appropriate method for transmitting sensitive or privileged information – think about whether you should use, for example, secure file transfer.

Instalcom staff must not make excessive use of the company's email facility for sending or receiving personal email. You must not pass on personal messages containing jokes, pictures or other similar attachments that could cause offence to any colleague and should discourage external contacts from sending such material. Subscribing or registering on websites using your Operating Company email address can lead to unwanted spam email being received and should be avoided where practical. Care must be taken when using email to avoid potential fraud and phishing attacks, which often involve identity theft. Instalcom staff should not click on links in emails unless they are sure of the source. Be wary of unusual emails from trusted sources.

Internet Usage Policy

All Operating Company staff are responsible for their use of the internet accessed through WPP or Operating Company systems.
Operating Company staff should neither copy, transmit nor download third party owned material without permission as this may infringe copyright.
WPP Data Privacy & Security Charter
Section 5: WPP ACCEPTABLE USE POLICY
Private & Confidential – 22 – © WPP

Operating Company staff must not use the internet to gain unauthorized access to computer systems.

Operating Company staff must not make excessive use of the Operating Company's internet connection for personal reasons during or outside working hours. Use of the internet may be monitored by the and you will be asked to justify excessive use of the facility. Operating Company staff must not attempt to access or retrieve offensive, pornographic, racist, violent, discriminatory or unlawful material or access any site that breaches the principles of the WPP Code of Conduct, local laws or could damage the reputation of WPP or the Operating Company. Operating Company staff that access these sites may be subject to disciplinary action up to and including dismissal.





IT POLICY

EMAIL USAGE POLICY

Instant Messaging

Instant Messaging Publicly available instant messaging (e.g. WhatsApp, Facebook Messenger) is not secure and its use should be avoided where possible for confidential, client and business-related communications. Such messaging platforms may be appropriate in respect of Business Continuity and Operating Companies should document how these platforms would be used as part of their Business Continuity Plan. Only OCG approved file sharing systems should be used. In the event employees use instant messaging services (e.g. WhatsApp) for work conversations, work product or business information, OCG reserves the right to access those messages to recover business or employee information stored there. Operating companies will inform employees that OCG may require access of such messages in these circumstances.

Use of Public File-Sharing Systems

There are a variety of publicly available and often free facilities to transfer large files without using email and to store data “in the cloud”. The use of such facilities should not be used for the transmission or storage of Operating Company data and/or client data. Only OCG approved filesharing systems should be used.

Signed.....Date: 03/01/22
Brian Lynch – Head of IT

Signed.....Date: 03/01/22
Vince Bowler - Managing Director