Electronic Communication & Devices Policy

STAR Group is committed to ensure appropriate behaviour and conduct when using Computer Networks, any form of electronic device and when contributing to electronic communication, websites, social media and applications by setting standards of use.

Objectives

- Comply with legislative requirements in relation to the use of electronic communications, Computer Networks and Devices
- Outline the expectations for using Star Group's Computer Network and Devices and what monitoring Star Group will perform and how records may be used

Application of Policy

This policy applies to anyone who may access Computer Networks ('Users') relating to the business operations of Star Group and to any employees or workplace participants who choose to contribute to social media sites.

This policy does not form part of your contract and may be varied at any time by Star Group.

Definitions

The following terms are used frequently throughout this policy:

'Device' refers to all electronic devices used for information display and communication. These include but are not limited to, laptop, tablet and desktop computers, printers, portable electronics, phones and associated equipment.

'Computer Network' refers to any network connections relating to the operations of Star Group, Internet connections, file storage, intranet and email facilities which are accessed by Star Group Devices.

'**Social Media'** refers to any public communication website or application that enables the sharing of views, comments, photographs or audio visual material. Some examples include but not limited to Facebook, Twitter, Instagram, LinkedIn, online platforms, discussion forums, blogs, chat rooms and messaging services.

'Content' refers to any texts, images, audio, videos, photographs, databases, documents or information that may be viewed by a Device and may be presented in the form of email, attachment, hardcopy, software, downloadable file, application or website.

'Streaming' refers to the playing of audio visual content via the Internet using websites or applications. Some examples include but not limited to YouTube, Netflix, Spotify, and Apple Music.

'Confidential Information' refers to any information that if disclosed to persons outside of the company, may be detrimental to Star Group's interests. This includes but is not limited to trade secrets and non-publicised information relating to the business and its affairs. Some examples are:

- pricing information, costs and rates, production scheduling, special supply information, project designs or project documentation,
- commercial, marketing, business or strategy plans, client contact lists and commercial details,
- exclusive supply arrangements, commission structures, contractual arrangements,
- tender policies, financial information; sales and training materials,
- technical data, schematics and designs, proposals and intentions,
- policies and procedures, and personal information covered by privacy laws.

'**Intellectual Property**' refers to all forms of intellectual property laws and rights including copyright, patent, design, trademark, trade name, and all confidential information.

Star Group's Computer Network

- Users must access Computer Networks with their assigned account credentials (username/password) and should not share their account credentials with anyone. The Computer Network is to be used for legitimate work purposes.
- Star Group expects you to take the approach that everything you do in connection with work, during and outside working hours, that involves:
  - sending emails
  - accessing and searching the internet (including Facebook, Twitter and any other social network, blogging or method of communicating via the internet)
  - using computer equipment issued or paid for by the Star Group

  is to be done in a professional and courteous manner.
- You should not expect that any email or other activity conducted over the Star Group computer network(s) will be private or otherwise confidential.
- Personal use is to be kept to a minimum and must not impact upon work performance, or that of other Users. Personal devices and visitors are permitted on 'Guest' Wi-Fi connections only, where available. 'Guest' Wi-Fi is monitored and content being accessed must comply with this Policy.
- Users must not access, transmit or save any Content or use the Computer Network in any way that may be deemed to:
  - be obscene, offensive or inappropriate;
  - cause insult, offence, intimidation or humiliation (e.g. material of a sexual nature, indecent or pornographic material);
  - be defamatory or damaging to Star Group's reputation;
  - be spam or dangerous to the Computer Network or other networks outside of Star Group;
  - interfere with business operations or Computer Network performance;
  - gain unauthorised access (hacking) within or outside the Computer Network;
  - facilitate personal gain or help personal business, such as running a personal business or crypto-currency mining;
  - make representations on behalf of Star Group without express authority to do so;
  - be illegal or relates to unlawful activity; or
  - compromise the security of the Computer Network.
- Only software and programs approved by the IT Department are to be used on Star Group Devices. Star Group is obligated to ensure all software and programs are appropriately licensed and compatible with the Computer Network. Software and programs that are protected by copyright and intellectual property laws are not to be copied or modified, except as permitted by law or by contract with the owner of the copyright.
- Disclosure of any Confidential Information via the Computer Network or Star Group Devices should be in accordance with Star Group's Documented Information Procedures.

- Modifications to the Computer Networks or Star Group Devices must only be undertaken by the IT Department.
- Star Group may prevent the delivery or access of Content or access to the Computer Network or Star Group Devices, if it is considered to be contrary to this Policy.
- Remote connectivity privileges to the Computer Network are granted to Users who require access when not physically connected to the Computer Network. Users may only connect to the Computer Network with Star Group Devices. Third party persons on occasion may need to connect to the Computer Network for system and application support, but must be approved by the IT Manager.
- Star Group offers no assurance of confidentiality or privacy for any personal information disclosed when using the Computer Network for personal purposes.

Computer Network and Device Monitoring

- Star Group engages in surveillance of the Computer Networks, Star Group Devices and Content on the Computer Network, including Content, location, email usage, internet usage and any other usage of information technology supplied by Star Group. This surveillance is carried out on an intermittent but ongoing basis and will effectively start upon commencement of this policy.
- Subject to legislative requirements, Content and Computer Network logs, information and archives are audited, monitored and remain the property of Star Group. They may be required as evidence in legal proceedings or workplace investigations relating to the conduct of a User, business activities or breach of this Policy.

Social Media

- Star Group acknowledges that Users may wish or be required to participate on social media platforms. Inappropriate use of social media may adversely affect Star Group's reputation, business operations, employees, clients and suppliers. For that reason, employees must not:
- expose Star Group to any possible legal liability (e.g. defamation or discrimination proceedings);
- identify or imply association with Star Group or publish Content which may reflect negatively on Star Group's reputation;
- disclose Confidential Information, or
- endorse or cite any client, partner or supplier without the permission of the Board of Directors.

Your Commitment

All Users must cooperate and comply with all policies, procedures and instructions in relation to Computer Networks, electronic communications and Devices. Users must be committed to:

- Immediately notify their manager should they become aware of any such Content on social media, a Device or the Computer Network, which is in breach of this Policy;
- Make all efforts to correct or remove erroneous or inaccurate Content on social media pertaining to Star Group;
- Not use Social Media during business hours, unless on designated breaks;
- Report suspicious electronic communications (i.e. emails or texts) or malicious Content to the IT Department;
- Not access another user's computer network facilities (including passwords and usernames/login codes) for any reason without the express permission of the user or Star;
- Not install software licensed to Star Group on personal devices;

- Not download, copy or save any Content relating to Star Group on a personal device or personal network.
- Not use business related Computer Networks to stream or download audio visual content for non-business purposes
- Use Star Group Devices for the performance of their role and respect, not misplace, protect and maintain in good order
- Not leave Devices unattended for extended periods of time. Devices are to be secured when not in use. Devices are not to be stored in an exposed position in vehicles.

CHRIS MULVEY
GROUP MANAGING DIRECTOR
01 July 2021