Fetch Metals

1. Technology, Internet, Email and Social Media Policy

1. Purpose and Scope

1.1 [COMPANY NAME] ('the Company') has developed this policy to protect the intellectual property, confidential information, brand, reputation, profitability and viability of the Company as well as the rights and interests of employees and clients.

1.2 This policy prescribes what the Company requires of its employees and contractors when using the computer systems, internet, email and social media on behalf of the Company or personally.

1.3 This policy applies to all Company employees and contractors acting on behalf of the Company.

1.4 This policy applies to all communications published by Company employees and contractors and all activities engaged in by employees and contractors on the internet that may have an impact on the business, brand or reputation of the Company, its employees or clients.

2. Social Media

2.1 Social media is the term given to websites and online tools that allow users to interact with each other by sharing or posting information, opinions, knowledge, interests and other content.

2.2 Examples of social media include:

- Social and business networking sites (such as LinkedIn and Facebook);
- Video and photo sharing websites (such as Instagram, TikTok and YouTube);
- Micro-blogging sites (such as Twitter);
- Forum and discussion boards (such as Reddit and Whirlpool Forums);
- Online encyclopaedias (such as Wikipedia); and
- Weblogs, including corporate blogs or personal blogs.

3. Personal Use of Social Media

3.1 The Company respects the right of employees and contractors to express personal views through social media.

3.2 Employees and contractors should be aware of the potential for communications on social media to adversely impact the business, brand,

reputation and rights of the Company, its employees and clients.

3.3 Employees and contractors must not use social media in a manner that may cause harm to the reputation of the Company.

3.4 When using social media in circumstances that are intended to be private or personal, employees and contractors must;

- make it clear that private opinions are their own and not say or do anything that may indicate they represent either the views of the Company or their connection with the Company;
- not publish anything harmful, obscene, abusive, offensive or illegal as a consequence of which harm may be caused to the Company, its employees or key stakeholders;
- not disclose information about the Company, its business, suppliers or clients that is confidential or likely to cause harm to the Company, its employees or key stakeholders;
- not use or disclose the Company's intellectual property; and
- comply with all laws including, but not limited to misleading and deceptive conduct, anti-discrimination, victimisation, vilification, privacy, intellectual property, anti-bullying, harassment and defamation.

4. Use of Social Media on Behalf of the Company

4.1 Employees using social media on behalf of the Company must be authorised by responsible senior management.

4.2 At all times when using social media for and on behalf of the Company, employees must comply with relevant training, directions, and guidance provided by the Company.

4.3 In addition, employees using social media on behalf of the Company must:

- avoid causing harm to the business, brand, reputation or rights of the Company, its employees, suppliers, clients or key stakeholders;
- use only authorised accounts; and
- immediately notify business unit management if they become aware of any possible breach of this policy or any incident which may adversely impact upon the Company.

4.4 In addition, employees using social media on behalf of the Company must not:

- disclose information that is confidential or commercially sensitive;
- disclose any confidential or other information about the Company or its business without appropriate approval; or
- breach any Company policy or any law.

5. Email Use

5.1 The Company's email accounts are not for private communication. The Company may, without reason or specific notice, access any email which is sent or received by a Company employee or a contractor who has been provided a Company email address.

5.2 Emails may also be isolated and automatically discarded if they possess any of the following characteristics:

- viruses;
- spam; or
- attachments considered a potential threat to the Company's systems. These include video clips, audio clips, executable program files, source code, image files in uncommon formats, and compressed or archived files.

5.3 Email facilities are provided for business purposes. Employees should be aware that when communicating via email, they are representing the Company. Good judgment, common sense and careful discretion is required.

5.4 The following types of emails are prohibited and should be deleted by employees immediately upon receipt;

- obscene, sexually explicit, pornographic, harassing, discriminatory, defamatory, inappropriate or objectionable messages or graphics;
- junk email messages;
- 'for profit' or spam messages; and
- 'chain letter' emails.

5.5 An employee who does not delete, or who forwards such emails to any third party either within the organisation or outside the organisation will be subject to disciplinary action and, depending upon the nature of the email, summary termination.

5.6 All emails using a Company email account should be drafted in appropriate, polite business language.

6. Internet Use

6.1 Internet access is provided to employees and certain contractors for business purposes related to their engagement with the Company. Occasional personal use is permissible but should be limited.

6.2 The Company may limit or prevent access to certain internet web sites.

6.3 Employees and contractors are prohibited from accessing:

- sites containing obscene, sexually explicit, pornographic, discriminatory, harassing, defamatory, or objectionable material;

- sites depicting or encouraging violence; or
- chat rooms.

6.4 Employees and contractors must seek permission from the IT department before downloading material from the internet onto a Company owned computer, due to the prevalence of viruses and other malicious content.

7. Monitoring

7.1 The Company considers any and all data created, stored or transmitted upon the systems (the Systems) as work product and, as such, expressly reserves the right to monitor and review any data upon the Systems, including your usage and history, on an intermittent basis without notice.

7.2 In addition to this, the Company has the right to protect its business interests and confidentiality. This includes the right to survey, audit and/or monitor its Systems, including but not limited to:

- monitoring sites users visit on the internet;
- monitoring time spent on the internet;
- reviewing material downloaded or uploaded; and
- reviewing emails sent and received.

7.3 Information reports will be available to the Company which can subsequently be used for matters such as system performance and availability, capacity planning, cost re-distribution and the identification of areas for personal development.

7.4 For the avoidance of doubt, we reserve the right to monitor all internet and email activity by you for the purposes of ensuring compliance with the Company's policies and

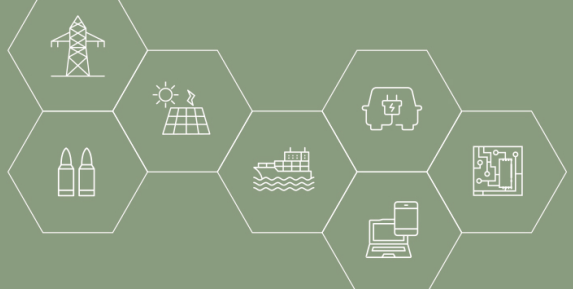
procedures and for ensuring compliance with the relevant regulatory requirements and you hereby consent to such monitoring.

7.5 Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

8. Use of Computer Equipment

8.1 In order to control the use of the Company's computer equipment and reduce the risk of contamination, the following rules will apply:

- the introduction of new software must first of all be checked and authorised by management before general use will be permitted;
- only authorised staff are permitted access to the Company's computer equipment;
- only software that is used for business applications may be used on the Company's computer equipment;
- no software may be brought onto or taken from the Company's premises without



prior authorisation;

- unauthorised access to computing facilities will result in disciplinary action up to and including dismissal; and
- unauthorised copying and/or removal of computer equipment and/or software will result in disciplinary action up to and including dismissal.

9. Discipline Policy

The Company's Discipline Policy applies to any breach of this policy.

File Name:	Technology, Internet, Email and Social Media Policy
Implementation Date:	[insert date]
Review Date:	[insert date]
Version:	1.0