Recorra Ltd – USE OF COMPUTER EQUIPMENT, EMAIL AND INTERNET POLICY

A. USE OF COMPUTER EQUIPMENT

1. Personal use of our computers

Our computers, including laptops, and PDAs, are to be used solely for business purposes, subject to the following exceptions:

You may make reasonable personal use of the Company's computer system and internet connection. You should do this mainly outside of your normal working hours or during your lunch break, in accordance with the terms of this policy. In order to control the use of the Company's computer equipment and reduce the risk of viruses the following will apply:

a. The introduction of new software must first of all be checked and authorised by a nominated senior member of the Company.

b. Only authorised staff should have access to the Company's computer equipment.

c. Only authorised software may be used on any of the Company's computer equipment.

d. Only software that is used for business applications may be used.

e. No software may be brought onto or taken from the Company's premises without prior authorisation.

f. Unauthorised access to the computer network will result in disciplinary action.

g. Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action. Such actions could lead to dismissal.

h. Proper care must be taken with Company laptops, data sticks etc when these are taken out of the office for any reason.

B. EMAIL AND INTERNET POLICY

1. Introduction

The purpose of the Internet and email policy is to provide a framework to ensure that there is continuity of procedures in the usage of internet and email within the Company. The internet and email system have established themselves as an important communications facility within the Company and have provided us with contact with professional and academic sources throughout the world. However, they also carry serious risks. Careless use of our email and internet system can have serious consequences. For example, it is possible to create a legally binding contract by exchange of email, or confidential information may be deliberately or accidentally sent to the wrong people.

In addition, misuse of the Internet and emails can introduce viruses into the network, infringe copyright laws and result in the harassment or defamation of others. For these reasons, we have to impose limits on Internet and email use in relation to both business and personal use. Therefore, to ensure that we are able to utilise the system to its optimum we have devised a policy that provides maximum use of the facility whilst ensuring compliance with the legislation throughout.

2. Email

The use of the email system is encouraged as appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims. When sending emails, internally or externally, you should exercise the same care as you would if you were sending a letter on our headed paper.

The procedure sets out the Company's position on the correct use of the email system.

Please note that all Emails sent or received on the Company system may be monitored. Should you wish to send/receive personal Emails of a private and confidential nature you should use your own personal email account.

3. Procedures - Authorised Use

a. Unauthorised or inappropriate use of the email system may result in disciplinary action which could include summary dismissal.

b. The email system is available for communication and matters directly concerned with the legitimate business of the Company. Employees using the email system should give particular attention to the following points:

i) all comply with Company communication standards.

ii) Email messages should be kept concise and copies should only be sent to those for whom they are particularly relevant.

iii) Email should not be used as a substitute for face-to-face communication or telephone contact. Abusive mails must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding.

iv) if email is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The Company will be liable for infringing copyright or any defamatory information that is circulated either within the Company or to external users of the system.

v) offers or contracts transmitted by email are as legally binding on the Company as those sent on paper. It is possible to create legally binding contracts without intending to via email correspondence. Email must not be used for communications that could lead to a binding contract being formed or which would have the effect of obligating the Company in any way, unless you have the clear authority to make the commitment in question.

Remember, a typed name at the bottom of an email is the same as a signature on a letter.

c. The Company will not tolerate the use of the email system for unofficial or inappropriate purposes, including:-

i) transmitting copyright information.

ii) passing on confidential information about other employees, the Company
or its customers or suppliers.

d. You must not send, forward, distribute or retain email messages that contain language that is abusive, aggressive, obscene or offensive. You must not make any improper or discriminatory reference to the protected characteristics of a person when writing emails and must not forward or distribute any material which does so. Protected characteristics are race, religion or belief system, sex, age, sexual orientation, gender-reassignment

and disability. Doing so may amount to gross misconduct. A good rule of thumb is to ensure that you never put something in an email that would offend or embarrass any reader or yourself. Always remember that an email might be seen by someone other than the intended recipient.

4. Internet

Where appropriate, duly authorised staff are encouraged to make use of the internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Company name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the Internet. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or non-related employment issues, leave an individual liable to disciplinary action which could lead to dismissal.

5. Inappropriate Websites

You must not under any circumstances access inappropriate or offensive websites or distribute or obtain similar material through the Internet or email when using our equipment, even in your own time. Examples of inappropriate or offensive material include racist material; pornography; sexually explicit images, text and related material; the promotion of illegal activity or intolerance of others. Doing so will amount to gross misconduct. In addition, you must not access gambling sites or pirated copyright material.

The Company retains the final decision as to whether it considers particular material to be inappropriate under this policy.

As a general rule, we would regard material to be inappropriate if any person in the Company might be offended by any of the contents or if the Company would be embarrassed if it were known that its software had accessed the particular web pages. If you are unsure whether we would consider particular material to be appropriate, do not access it or distribute it.

If you receive material which contains or you suspect contains inappropriate material or you inadvertently access such material on the Internet, you must immediately report this to your Line Manager. Do not under any circumstances forward the material, show it to anyone else or otherwise distribute it.

6. Virus Protection Procedure

The introduction of a virus into our computer system could be devastating. We have installed antivirus software but this does not guard against all viruses. You should be aware that viruses can be introduced via email attachments, USB memory sticks and the Internet.

In order to prevent the introduction of virus contamination into the software system the following must be observed: -

a. It is your responsibility to take care when opening email attachments, especially when they are not expected or they are from unknown sources. If you are in any doubt about an attachment, please contact Transpeed who will check whether it is safe to open the attachment. You must never open attachments ending with '.exe' without first obtaining clearance from Transpeed.

b. You should not install any software that has not been approved or purchased by the Company, nor should you download any material, including games and screen savers, from the Internet or USB memory sticks without first obtaining the approval of Transpeed.

C. SECURITY

You are responsible for the security of the equipment allocated to you and must not allow it to be used by anyone other than in accordance with this policy.

1. Wireless technology

Everyone who has a Company laptop will be advised by Transpeed whether it can be used via wireless technology. This is only allowed if the appropriate security software and encryption are in place.

2. Travelling

Given the amount of confidential information which is accessible on our equipment, you must take sensible precautions when you take laptops and PDAs out of the office. In particular, you must never leave one of our laptops or PDAs on view inside a vehicle. If you have to leave such an item unattended in a vehicle, it must be locked away in the boot or glove compartment. If you are travelling on public transport or are in a public place, keep your laptop or PDA with you at all times or, if this is not possible, in sight. Remember that thieves specifically target laptop-carrying cases.

If you are working in a public place, be aware that other people may be able to read documents that you are working on.

3. Passwords

You should not use another person's password without authorisation and you should not tell anyone (other than Transpeed or your Line Manager) your password, unless there is a pressing business need to do so. You must log out of your computer when you are not using it and when you leave the office. For the avoidance of doubt, on termination of your employment for whatever reason, you must provide details of all your passwords.

4. Email security

It is very easy to send an email to the wrong person. You should be very careful to ensure that the emails you send are correctly addressed, particularly when they contain information that you would not want others to see.

Remember that email is not a secure way of sending information. Emails can be intercepted by third parties and intended recipients can alter and/or forward emails without your knowledge. You should therefore avoid sending by email personal information about individuals or commercially sensitive information.

Remember that deletion from your inbox or archives does not mean that emails are destroyed, and at times we may need to retrieve them. Email messages may be disclosed in legal proceedings in the same way as paper documents.

D. MONITORING COMMUNICATIONS

1. How do we monitor communications?

We log and audit the use of:

a. telephones, including mobile telephones, and fax machines

b. computers, laptops and PDAs, including email, Internet and other computer use

c. personal mobile telephones and landlines if we pay for them or contribute towards their cost

All calls from all extensions and from Company mobile telephones are logged and regularly audited. Auditing software has been installed to monitor email traffic and any Internet sites visited. We keep back-up tapes that record computer usage which are retained for 12 months.

Where we have good reason, we may monitor and record the contents of telephone calls, voicemail messages, faxes, computer files, Internet use and emails sent, received and stored. We will always act within the law. You should also be aware that your emails and voicemails will be checked during times when you are absent from work. Given this, you should not regard either business or personal communications on our facilities as private.

2. Purposes of monitoring

The purposes of such logging, auditing, monitoring and recording are to:

a. ensure the effective operation of our telecommunications systems and to maintain system security, including the retrieval of lost messages

b. investigate and detect unauthorised use of the systems in breach of this policy, such as excessive personal use or distribution of inappropriate material

c. check whether any matters need to be dealt with in your absence

d. investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or a third party

e. pursue any other legitimate reason relating to the operation of the business

This list is not exhaustive.

The information gathered will only be given to those who need to see it in accordance with these purposes. If information gathered is relevant to any disciplinary action taken, it will be made available to those who are involved in the disciplinary procedure.

E. SOCIAL MEDIA POLICY

1. Purpose and Scope

This policy covers all forms of social media, including Facebook, LinkedIn, Twitter, Google+ Wikipedia, other social networking sites, and other internet postings, including blogs. It applies to the use of social media for both business and personal purposes, during working hours and in your own time to the extent that it may affect the business of the Company. The policy applies both when the social media is accessed using our Information Systems and also when access using equipment or software belonging to employees or others.

Whilst we recognise the benefits which may be gained from appropriate use of social media, it is also important to be aware that it poses significant risks to our business. These risks include disclosure of confidential information and intellectual property, damage to our reputation and the risk of legal claims. To minimise these risks this policy sets out the rules applying to the use of social media.

This policy covers all employees of the Company. Breach of this policy may result in disciplinary action up to and including dismissal. Any misuse of social media should be reported to the Marketing Manager and the HR Manager. Questions regarding the content or application of this policy should be directed to the Marketing Manager or the HR Manager. This policy is not contractual and we may amend it at any time if we consider it appropriate to do so.

2. Personal use of social media at work

You are not permitted to access any social media for your personal use during working time or using our Information Systems at any other time. We may monitor your use of its systems, including use of social media sites.

3. Business use of social media

You may, and are encouraged to, share content by the company's official business page.

If you are required or permitted to use social media sites in the course of performing your duties for or on behalf of us, you should ensure that such use has appropriate authorisation and that it complies with the standards set out in this policy.

4. Responsible use of social media

You must not use social media in a way that might breach any of our policies, any express or implied contractual obligations, legislation, or regulatory requirements. In particular, use of social media must comply with:

a. the Equal Opportunities and Personal Harassment policies

b. rules of any relevant regulatory bodies

c. contractual confidentiality requirements

d. other key policies/requirements.

In your use of social media, you must not:

a. make disparaging or defamatory statements about us, our employees, clients, customers, or suppliers;

b. harass, bully or unlawfully discriminate in any way;

c. use data obtained in the course of your employment with us in any way which breaches the provisions of the Data Protection Act 2018;

d. breach copyright belonging to us;

e. disclose any intellectual property, confidential or commercially sensitive information relating to our business;

f. make statements which cause, or may cause, harm to our reputation or otherwise be prejudicial to our interests.

You should avoid using social media communications that might be misconstrued in a way that could damage our business reputation.

You should make it clear in personal postings that you are speaking on your own behalf, in particular write in the first person and use a personal e-mail address.

If you disclose that you are an employee of ours, you must state that your views do not represent those of your employer. For example, you could state, *"the views in this posting do not represent the views of my employer"*. Remember that you are personally responsible for what you communicate in social media.

If it is unclear where we stand on certain "hot" topics you are obligated to ask the Marketing Manager for clarification before sharing any content on social media. They hold the right to deny any posting or sharing of content of a particular topic if they believe it will publicly oppose the business's position.

Often, materials published will be widely accessible by the public and will remain accessible for a long time. If you are uncertain or concerned about the appropriateness

of any statement or posting, you should discuss it with the Marketing Manager before making the post.

5. Monitoring of Social Media Use

It is recommended that all employees use strict privacy settings on their social network profiles.

The organisation monitors your internet usage regularly and may undertake more in depth monitoring where considered necessary. This includes monitoring the websites you visit and any other matters referred to in this policy. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account.

6. Enforcement

Any employee who we suspect has breached this policy will be subject to the organisation's disciplinary procedure.

Signed:  Date: 1/4/2024

MANAGING DIRECTOR

Recorra includes Recorra Ltd and its subsidiaries. Recorra was formerly known as BPR Group which included Paper Round, Secure Paper, Brighton Paper Round Ltd and Reef Environmental Solutions Ltd.