wentworth

Internet, email and communications policy and procedures

February 2021

INTERNET, EMAIL AND COMMUNICATIONS POLICY AND PROCEDURES

1. INTRODUCTION

1.1 The Company recognises that the use of email and the internet can save time and expense, and is an important part of the way we work. However, it brings with it certain risks, some of which may involve potential legal and financial liabilities for both the Company and the individual, e.g.:

1.1.1 inadvertently entering into contracts or commitments on behalf of the Company;

1.1.2 introducing viruses into the Company's systems;

1.1.3 breaching copyright or licensing rights;

1.1.4 breaching data protection rights;

1.1.5 breaching confidentiality and security;

1.1.6 defamation; and/or

1.1.7 bullying, harassment and discriminatory conduct.

1.2 This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

1.3 This policy provides important information about:

1.3.1 the Company's rules on the use of internet, email, telephone and other communications systems at work, including in relation to confidentiality, security and personal use;

1.3.2 how the Company monitors the use of those systems;

1.3.3 your rights and obligations in relation to data protection;

1.3.4 the consequences of failure to comply with this policy; and

1.3.5 review and training.

1.4 Once you have read and understood this policy, please confirm that you have done so by signing and returning the attached copy to your Manager.

1.5 References in this policy to 'email' apply equally to other electronic communications, messaging tools and posts.

1.6 Corporate HR & Administrative Manager is responsible for the monitoring and implementation of this policy. Any questions about the content or application of this policy or other comments should be referred to Corporate HR & Administrative Manager in the UK or the HR and Administration Manager in Tanzania.

2. SCOPE

2.1 This policy applies to:

2.1.1 all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, and to consultants and other contractors who have access to our computer and other communications systems;

2.1.2 personal use of our systems and equipment in any way that reasonably allows others to identify any individual as associated with the Company;

2.1.3 the use of our email, telephone and internet systems both in the workplace and from outside it, e.g. via remote access, and to the use of a Company laptop, tablet, mobile phone, smartphone or personal digital assistant (PDA).

2.2 You must familiarise yourself with this policy and comply with its terms.

2.3 You should also refer to our Data Protection Policy and Privacy Policy and, where appropriate, to our other relevant policies.

2.4 We will review and update this policy regularly in accordance with changes in technology, the law and current business practice. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

3. USE OF THE COMPANY'S COMPUTER AND COMMUNICATION SYSTEMS

3.1 You may use our computer and communication systems (including equipment) for authorised purposes only, i.e. for the purposes of our business or in accordance with paragraph 11 (permitted personal use). If you wish to use the Company's systems or equipment for another purpose, you must obtain express permission from your line manager before doing so.

3.2 To reduce the risk to the Company's systems or network of virus infections, hacking and other unauthorised access attempts, you may only access the Company's systems and network as follows:

3.2.1 from your workplace or other Company premises, using authorised equipment only;

3.2.2 remotely via broadband, dial up, etc, using authorised equipment via secure means, e.g. VPN software only;

3.2.3 remotely, using unauthorised equipment, e.g. your home computer or an internet café terminal, via Windows Virtual Desktop;

3.2.4 remotely from authorised and unauthorised mobile devices, e.g. mobile phones and tablets, via authorised applications, e.g. Outlook Mobile, where the Company's mobile device management agent has been installed and access is MFA protected.

3.3 We license software from a number of sources. We do not own that software and must comply with any restrictions or limitations on use, in accordance with its licence agreements. You must adhere to the provisions of any software licence agreements to which we are party.

3.4 You must not use any software owned or licensed by the Company for any purpose other than those of our business without express permission from your Manager or as otherwise permitted by the terms of this policy, and you must not copy, download or install any software without first obtaining express permission from the IT Support Desk and your Manager.

4. EMAIL USE—GENERAL

4.1 All communications, including email, should reflect the highest professional standards at all times. In particular, you must:

4.1.1 keep messages brief and to the point;

4.1.2 check emails carefully before sending, including spelling and grammar;

4.1.3 ensure that all emails sent from the Company include the current disclaimer wording;

4.1.4 ensure that an appropriate heading is inserted in the subject field; and

4.1.5 check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about the Company, a client/customer or other third parties.

4.2 You must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

4.3 You must not send or post messages or material that are offensive, obscene, defamatory or otherwise inappropriate in the work environment. This includes, but is not limited to messages that:

4.3.1 are inconsistent with our Code of Ethics and Business Conduct;

4.3.2 criticise our competitors or their staff;

4.3.3 suggest that there are quality problems with goods or services of suppliers, clients or customers; or

4.3.4 state that anyone is incompetent.

4.4 You must not send or post any message or material which could be regarded by the recipient or any other person as personal, potentially offensive or frivolous.

4.5 Equally, if you receive a message that is offensive, obscene, defamatory or inappropriate in the work environment, you must delete it immediately and not forward it to any internal or external recipient, other than internally to Corporate HR & Administrative Manager in the UK or the HR and Administration Manager in Tanzania in order to report a breach of this or another Company policy.

4.6 You should not send or post anything in an email that you would not be comfortable writing (or someone else reading) in a letter. Emails leave a retrievable record and, even when deleted, can be recovered from our back-up system or an individual's computer. They are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases, and they can also be reviewed by regulators.

4.7 You must not create congestion on the Company's systems or network by sending trivial messages, by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

4.8 You must use a Company email address for sending and receiving work-related emails and must not use your own personal email accounts to send or receive emails for the purposes of our business. You must not send (inside or outside work) any message in our name unless it is for an authorised, work-related purpose.

4.9 You must not send unsolicited commercial emails to anyone with whom you do not have a prior relationship without the express permission of the relevant manager.

4.10 Emails containing personal data or special categories of personal data may be retained only in accordance with our records retention policy. Customer-related emails should be attached to our document management system within 48 hours of receipt. If an individual need to keep any emails that are not customer-related, these should be stored in personal folders.

4.11 You must be vigilant when using our email system. Computer viruses are often sent by email and can cause significant damage to the Company's information systems or network. Be particularly cautious in relation to unsolicited emails from unknown sources.

4.12 If you suspect that an email may contain a virus, you should not reply to it, open any attachments to it or click on any links in it and must contact the IT Support Desk immediately for advice.

5. EMAILS—CONFIDENTIALITY

5.1 Do not assume that emails sent or received internally or externally are private and confidential, even if marked as such. Email is not a secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential. The confidentiality of internal communications can only be ensured if they are sent by internal post, delivered personally by hand or included in a password-protected or encrypted online document.

5.2 You should refer to your contract and the Staff Handbook for details of the types of information that we regard as confidential and which should be treated with particular care.

5.3 Lists of contacts compiled by you during the course of your employment and stored on our email application, information manager and/or other database(s) (irrespective of how they are accessed) belong to us. You must not copy or remove such lists for use outside your employment or after your employment ends.

6. EMAILS—PERSONAL USE

6.1 Although the email system is primarily for business use, we understand that you may occasionally need to send or receive personal emails while at work.

6.2 The sending of personal emails using the work email address is therefore permitted. When sending personal emails using the work email address, you should show the same care as when sending work-related emails.

6.3 Reasonable personal use of our systems or network to send personal email is also permitted, provided that it does not interfere with the performance of any individual's duties and the terms of this policy are strictly adhered to. We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

6.4 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

6.4.1 it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, i.e. during lunch or other breaks, or before and after work;

6.4.2 personal use must not affect the job performance of you or your colleagues, or otherwise interfere with our business; and

6.4.3 it must not commit us to any marginal costs.

7. EMAILS—MONITORING

7.1 We may monitor the email and instant messaging systems or network in the workplace for the following reasons:

7.1.1 to determine whether they are communications relevant to the carrying on of our business;

7.1.2 if you are absent from work, to check communications for business calls to ensure the smooth running of the business;

7.1.3 to record transactions;

7.1.4 where we suspect that messages being sent or received are:

(a) detrimental to the Company;

(b) in breach of an individual's contract, or this policy;

(c) in breach of data protection rights;

7.1.5 to monitor staff, conduct;

7.1.6 to investigate complaints, grievances or criminal offences.

7.2 When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

7.2.1 look at the sender or recipient of the email and the subject heading only; and

7.2.2 avoid opening emails marked 'Private' or 'Personal'.

7.3 We do not as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of our systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon us. To achieve these objectives, we carry out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals.

7.4 We will only intercept (i.e. open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our business and where necessary:

7.4.1 to determine whether the message is relevant to the carrying on of our business;

7.4.2 to establish the existence of facts;

7.4.3 to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, i.e. to detect unauthorised use of the system;

7.4.4 to check whether staff using the system in the course of their duties are achieving the standards required of them;

7.4.5 for the purpose of investigating or detecting the unauthorised use of the system;

7.4.6 for the purpose of preventing or detecting crime; or

7.4.7 for the effective operation of the telecommunication system.

7.5 The content of emails will be examined only in exceptional circumstances, initially by the IT Support Desk and the Corporate HR & Administrative Manager. The information obtained through monitoring may be shared internally, with members of the HR department and your line manager, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the IT team believes there may have been a breach of the individual's contract or this policy.

8. TELEPHONES—PERSONAL USE

8.1 Although the telephone system is primarily for business use, we understand that you may occasionally need to make or receive personal telephone calls while at work.

8.2 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

8.2.1 it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, i.e. during lunch or other breaks, or before and after work;

8.2.2 it must not affect the job performance of any member of staff or otherwise interfere with our business;

8.2.3 it must not commit us to any marginal costs; and

8.2.4 you may not use the telephone during working hours to perform work for yourself or another employer, or to look for work; or

8.2.5 you may not communicate confidential information other than in the course of your duties, or act in a way that is detrimental to the Company.

8.3 Our telephone system may not be used for premium rate or international calls for personal use unless expressly authorised by the individual's manager. Where possible, business calls should be made using Zoom, Teams or other low cost medium.

9. TELEPHONES—MONITORING

9.1 We may monitor the use of our telephone system, and Company mobile phones (including smartphones) for the following reasons:

9.1.1 if you are absent from work, to check communications (including your voicemail) for business calls to ensure the smooth running of the business;

9.1.2 to record transactions;

9.1.3 where we suspect that an individual is acting in a way that is:

(a) detrimental to the Company;

(b) in breach of the individual's contract, or this Policy;

(c) in breach of data protection rights;

9.1.4 to monitor staff, conduct;

9.1.5 to investigate complaints, grievances or criminal offences.

9.2 When monitoring telephones, we will, unless exceptional circumstances apply, look at the numbers from which calls are received and the numbers dialled and the duration and frequency of calls.

9.3 We will only intercept (i.e. listen to) telephone calls or saved messages where relevant to the carrying on of our business and where necessary:

9.3.1 to determine whether the message is in fact relevant to the carrying on of our business;

9.3.2 to establish the existence of facts;

9.3.3 to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, i.e. to detect unauthorised use of the system;

9.3.4 to check whether staff using the system in the course of their duties are achieving the standards required of them;

9.3.5 for the purpose of investigating or detecting the unauthorised use of the system;

9.3.6 for the purpose of preventing or detecting crime; or

9.3.7 for the effective operation of the telecommunication system.

9.4 Telephone calls will be intercepted only in exceptional circumstances, initially by Corporate HR & Administrative Manager in the UK or the HR and Administration Manager in Tanzania. The information obtained through monitoring may be shared internally, with members of the HR department and your line manager, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the IT department believes there may have been a breach of the individual's contract or this policy.

10. INTERNET—GENERAL

10.1 Access to the internet during working time is primarily for matters relating to your work duties and employment. Reasonable, limited personal use of the internet is permitted in accordance with paragraph 11.

10.2 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):

10.2.1 creating, viewing or accessing any webpage, or posting, transmitting or downloading any image, file or other information that is unrelated to your employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us, our business partners or to our clients/customers and/or suppliers;

10.2.2 engaging in computer hacking and/or other related activities; and

10.2.3 attempting to disable or compromise security of information contained on our systems or network or those of a third party.

10.3 Staff are reminded that such activity may also constitute a criminal offence.

10.4 Postings placed on the internet may display our address. For this reason, you should make certain before posting information that the information reflects our standards and policies. Under no circumstances should information of a confidential or sensitive nature be placed on the internet. You must not use the Company's name in any internet posting (inside or outside work) unless it is for a work-related purpose.

10.5 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. You must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.

10.6 You must not commit us to any form of contract through the internet.

10.7 Subscriptions to news groups, mailing lists and social networking websites are permitted only when the subscription is for a work-related purpose and has been approved by your Manager. Any other subscriptions are prohibited.

10.8 We may block or restrict access to any website at its discretion.

11. INTERNET—PERSONAL USE

11.1 Reasonable personal use of our systems or network to browse the internet is allowed provided that it does not interfere with the performance of your duties and the terms of this policy are strictly adhered to. We reserve the right, at its absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

11.2 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

11.2.1 it must be minimal (both in terms of time spent and frequency) and reasonable and must take place mainly outside normal working hours, i.e. during lunch or other breaks, or before and after work;

11.2.2 it must not affect the job performance of any member of staff or otherwise interfere with our business; and

11.2.3 it must not commit the Company to any marginal costs.

12. INTERNET—MONITORING

12.1 We may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that an individual has been using the internet in breach of the contract of employment or this policy, e.g.:

12.1.1 by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us or to our clients/customers;

12.1.2 by spending an excessive amount of time viewing websites that are not work-related.

12.2 Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using Company systems or network and internet usage using hand-held or portable electronic devices.

12.3 Monitoring will normally be conducted by Corporate HR & Administrative Manager in the UK or the HR and Administration Manager in Tanzania in conjunction with the IT Support Desk. The information obtained through monitoring may be shared internally, with members of the HR department and your line manager, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the Corporate HR & Administrative Manager in the UK or the HR and Administration Manager in Tanzania in conjunction with the IT Support Desk believes there may have been a breach of the individual's contract or this Policy.

13. PASSWORDS AND SECURITY

13.1 You are personally responsible for the security of all equipment allocated to or used by you. You must not allow equipment allocated to you to be used by any other person, other than in accordance with this policy.

13.2 You must use passwords on all IT equipment allocated to you, and keep any password allocated to you confidential and change your password regularly.

13.3 All external access must be protected by Multi factor Authentication (MFA).

13.4 You must not use another person's username and/or password to access our systems or network, nor allow any other person to use your password(s). If it is anticipated that someone may need access to your confidential files in your absence, you should arrange for the files to be copied to a network location that is properly secure where the other person can access them or give the person temporary access to the relevant personal folders.

13.5 You must log out of the system or lock your computer when leaving your desk for any period of time. You must log out and shut down your computer at the end of the working day.

14. COMPANY SYSTEMS AND DATA SECURITY

14.1 You must not download or install software from external sources without prior authorisation from the IT department.

14.2 You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other device to our systems or network without express prior permission from the IT department. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this.

14.3 You must not run any '.exe' files, particularly those received via email, unless authorised to do so in advance by your Manager and the IT Support Desk. Unauthorised files should be deleted immediately upon receipt without being opened.

14.4 You must not access or attempt to access any password-protected or restricted parts of our systems for which you are not an authorised user.

14.5 You must inform the IT department immediately if you suspect your computer may have a virus and must not use the computer again until informed it is safe to do so.

14.6 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

15. PROHIBITED USE AND BREACH OF THIS POLICY

15.1 We consider this policy to be extremely important. Any breach of the policy will be dealt with under our Disciplinary Procedure. In certain circumstances, breach of this policy may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw your internet and/or email access.

15.2 Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

15.2.1 unauthorised use of the internet as outlined in paragraph 10.2 above;

15.2.2 creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;

15.2.3 creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our Code of Ethics and Business Conduct Policy;

15.2.4 accessing, transmitting or downloading any confidential information about us and/or any of our staff and/or client or customers, except where authorised in the proper performance of your duties;

15.2.5 accessing, transmitting or downloading unauthorised software; and

15.2.6 viewing, accessing, transmitting or downloading any material in breach of copyright.