

Email, Telephone, Computer Facilities and Social Media Policy

2018

valwade
RECRUITMENT



Purpose of this policy

This policy sets out the Company's policy for use of its Facilities and Networking Sites and covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, home workers, part-time and fixed-term employees, casual and agency staff, temps, and volunteers. ("You"). "Your" and "Yourself" shall be construed accordingly and where there are references to "employee" and/or "your employment" throughout this document, these should be read as referring to the terms upon which you are either employed or engaged by the Company (as applicable). Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy. This policy shall apply during the course of your employment including any period of garden leave (and where stated, also after your employment has ended). [see Note 1]

Definitions

Use of the Facilities

- Work use of the Facilities
- Personal use of the Facilities
- Prohibited use of the Facilities

Use of Networking Sites

- Professional Networking Sites
- Rules for using Professional Networking Sites
- Contacts made via Professional Networking Sites
- Maintenance of the Company profile on Professional Networking Sites
- Social Networking Sites
- Post termination of employment or engagement restrictions

How to use the Facilities, and Networking Sites

- Information recipients
- Content and tone of communications
- Out of Office messages
- Deleting or archiving material
- Suspect material, documents or viruses
- Passwords

Monitoring use of the Facilities and Networking Sites

Unsolicited communications

Termination of employment with the Company

Status of this policy

Acknowledgement of receipt of this policy

Definitions

"Confidential Information" means:

information relating to the Company's business plans, finances, new or maturing business opportunities, and research and development projects;

marketing information relating to the Company's marketing or sales of any past, present or future service including without limitation sales targets and statistics, market share and pricing statistics, marketing surveys and plans, market research reports, sales techniques and price lists;

details of Professional Contacts including names, addresses, contact details, terms of business or proposed terms of business with them, their business requirements, pricing structures, lists of employees and their terms of employment;

and

any other information of a confidential nature belonging to employees, candidates, clients, and employees of clients of the Company or in respect of which the Company owes any other obligation of confidence.

"Facilities" means telephone and computer facilities, including email and the internet, and hardware including mobile media such as laptops, mobile phones, BlackBerries™, smartphones, personal digital assistants, iPads™, tablets or notebooks, or similar equipment.

"Networking Sites" includes (but is not limited to) professional networking sites such as LinkedIn, Xing, Viadeo ((Professional Networking Sites) and social networking sites such as Facebook, Twitter, SecondLife, Google+, Wikipedia, (Social Networking Sites). Your access to and use of Networking Sites, whilst employed by the Company is set out in this policy. [see Note 2]

“Personal Contacts” means any of Your friends (not including Professional Contacts).[see Note 3]

“Professional Contacts” means any Candidate, Client, Introducer, Key Employee, Prospective Candidate or Prospective Client (all as defined in Annex 1), together with any contacts made through a professional body trade or association of which You or the Company is a member. [see Note 3]

Use of the Facilities:

Work use of the Facilities

The Facilities are made available to You during the course of your employment with the Company to assist You in carrying out and promoting the Company’s business and interests.

Personal use of the Facilities

The Facilities [may OR may not] be used[, within reason,] for personal communications or to send and retrieve personal messages and to browse external web-sites for personal use [although this should be done outside office hours and be kept to a reasonable limit. It must not interfere with business commitments. If there is any evidence that this privilege is being abused then the privilege [may/ will] be withdrawn]. The content of personal e-mails must also comply with the restrictions set out in section 3.3 of this policy. If using the Facilities for personal communications You should be aware that the Company may monitor your use of the Facilities in accordance with section 6 of this policy and any breaches of this policy may result in disciplinary action up to and including dismissal. [see Notes 4 and 12]

Prohibited use of the Facilities

The following uses of the Facilities are expressly prohibited:

- viewing internet sites which contain pornographic, obscene, abusive, slanderous or otherwise offensive material or downloading or forwarding such material within or outside the Company;
- sending, receiving or forwarding communications that are in violation of company policy including, but not limited to, the transmission of obscene, offensive or harassing messages;
- sending receiving or forwarding communications which make unsubstantiated and potentially defamatory comments about colleagues, clients, candidates or any other person via the Facilities or any Networking Site. You are reminded that communications via social media constitutes publication just as printing in hard copy or via email is publication. You personally, and/ or the Company could face a defamation action should you publish unsubstantiated and potentially defamatory material;
- sending, receiving or forwarding communications that disclose Confidential Information without the prior authorisation of [the Company’s IT Manager/ your line manager/ or other];
- bullying or harassing colleagues, clients, candidates or any other person via the Facilities or any Networking Sites
- discriminating or making offensive or derogatory comments about any colleagues, clients, candidates or any other person via the Facilities or any Networking Site;

- breaching any other Company’s policies including in particular, but not limited to, the Information Security and Data Protection Policy, the Equal Opportunities and Diversity Policy and [any other];

- engaging in any behaviour which might cause either the Company to be in breach of the REC Code of Professional Conduct or You to be in breach of the Institute of Recruitment Professionals’ Code of Ethics (if You are a member of that Institute);

- duplicating copyrighted or licensed software or other information without the appropriate authorisation;

- installing or downloading any software or hardware without the specific approval of the [Company’s IT Manager/ Managing Director/ other] or other person delegated by him/ her to give such approval;

- forwarding or otherwise perpetuating junk mail or “chain-letter” type e-mail within or outside the Company;

- removing any hardware or software from the Facilities or the Company’s premises without prior approval of the [Company’s IT Manager/ Managing Director/ other]; and

- selling or advertising anything via the Facilities or broadcast messages about lost property, sponsorship or charity appeals, without the written agreement of your line manager.

If you engage in any prohibited activities this may result in the Company taking action against You under the Company’s Disciplinary, Dismissal and Grievance Procedures and which ultimately could lead to the termination of Your employment.

Use of Networking Sites:

Networking Sites are a valuable business tool which the Company wishes to use to build its brand, reputation and business [see Note 5], and which it recognises You may wish to use to build Your own professional reputation. However, in addition to the benefits there are also certain risks attached to using Networking Sites including but not limited to the Company’s Confidential Information, reputation and compliance with their legal obligations. In order to reduce those risks, for both Yourself and the Company, where and when You are representing the Company You must comply with conditions set out in this policy. Failure to comply with this policy may result in the Company taking action against you under the Company’s Disciplinary and Grievance Procedure.

Professional Networking Sites

The Company may provide You with access to Professional Networking Sites. Such access is granted for work-related purposes only and should be done for the benefit of the Company alone, though professional networking activity may be done inside or outside of working hours.

Rules for using Professional Networking Sites

The following rules apply when You access or use a Professional Networking Site: [set out here how your organisation authorises account opening e.g.]

- You must have written permission from [the Company’s IT Manager/ Your line manager/ or other] before setting up an account for any Professional Networking Site.

- You should create the account on the Professional Networking Site using your work email address only.
- You must notify [the Company's IT Manager/ Your line manager/ or other] of the details of your account including the password. Your password is confidential and should not be disclosed to any unauthorised person.
- You should only use the account for the purpose for which it was authorised. [If you are commenting on a Professional Networking Site on behalf of the Company you must seek approval from [state who] before submitting that comment.]
- You shall inform the Company of activities that you carry out in relation to Professional Networking Sites including details of your membership of sites that you have set up and new contacts that you have made during the course of your employment.
- You must regularly backup your Professional Contacts.
- You must regularly upload Professional Contacts to the Company's database(s).
- You should not disclose Confidential Information unless You have been authorised to disclose by [Your line manager/ the Managing Director/ the Finance Director/ other].
- You must comply with the terms and conditions of use of all Networking Sites that You use. You should pay particular attention to any codes of behaviour or professional conduct contained within those terms and conditions. [see Note 6]

REC Corporate members are also required to comply with the Code of Professional Practice and individual recruiters with the Code of Ethics of the Institute of Professional Recruiters. [see Note 7]

- You must advise the Company if you become aware of any breach of this policy by a colleague. Failure to do so may be a disciplinary offence. [see Note 8]

The Company reserves the right to restrict your access to Professional Networking Sites and accounts that the Company has created for you.

Contacts made via Professional Networking Sites

If You already have an account with any Professional Networking Site which contains Confidential Information belonging to the Company You must transfer that Confidential Information to a new account set up in accordance with section 4.1.1 of this policy. [see Note 9] Such account shall be subject to the rules set out in section 4.1.1 of this policy and the following additional rules:

- You must keep Personal Contacts separate from Professional Contacts.

The Company reserves the right to require You to provide evidence and details as to when You made your contacts and in which capacity they were made. You will be required to give access to your account(s) to [the Company's IT Manager/ Your line manager/ or other] for this purpose. The Company's decision on whether a contact constitutes a Personal or Professional Contact shall be final.

Maintenance of company profile on Professional Networking Sites

Certain Professional Networking Sites contain company profile pages relating to the Company. For the avoidance of doubt, these profile pages may only be edited by authorised users. Amendment of the Company's profile pages by unauthorised users shall be a disciplinary offence (and for this purpose You are referred to the Company's Disciplinary, Dismissal and Grievance Procedures).

If you are authorised to make a comment on a Professional Networking Site you must state clearly that these are personal views and not the views of the Company. [see Note 10]

Use of Social Networking Sites

The Company respects Your right to a private life [A: and therefore You may access social networking sites using the Facilities. However this should be done outside office hours and be kept to a reasonable limit. If there is any evidence that this privilege is being abused then the privilege may be withdrawn OR B: but access to social networking websites via the Facilities and during working hours is strictly forbidden [unless prior authorisation is obtained from [the Company's IT Manager/ Your line manager/ or other].

Your use of Social Networking Sites may impact on the Company and its business. Such impact includes potentially causing damage to its reputation, loss of Confidential Information, or exposure to other liabilities such as claims of discrimination, harassment or workplace bullying. The content of any communications or comments posted on a Social Networking Site must not damage or bring into disrepute the Company, its staff, clients or candidates. Therefore if You use Social Networking Sites, even where this is not via the Facilities or is outside of working hours You are prohibited from:

[identifying Yourself as working for the Company;] [see Notes 11 and 12]

- engaging in any conduct or posting any comments which are detrimental to the Company;
- engaging in any conduct or posting any comments which could damage working relationships between members of staff, Introducers, suppliers, affiliates, Clients and Candidates of the Company. Where you express personal views You must state that these are personal views and do not represent the views of the Company;
- engaging in any conduct or posting any comments which could be derogatory to another person or third party or which could constitute unlawful discrimination or harassment;
- recording any Confidential Information regarding the Company on any social networking site or posting comments about any Company related topics such as the Company's performance; and/ or
- making information available which could provide any person with unauthorised access to the Company, the Facilities and/or any Confidential Information.

You may be required to remove postings deemed to constitute a breach of this policy. This may include any 'likes' or 'dislikes' of other people's posts or the re-posting/tweeting of other people's comments (or links thereto) which of themselves may constitute a breach of this policy.

Post termination of employment or engagement restrictions

For the avoidance of doubt, the restrictions on the use of Networking Sites continue to apply throughout Your employment with the Company including any period of garden leave you may serve.

How to use the Facilities and Networking Sites

Information recipients

You must exercise caution when using the Facilities and any Networking Sites. In addition to the restrictions set out in sections 3 and 4 of this policy, care must be used in addressing emails, postings on Networking Sites or other electronic communications to make sure that they are not sent to the wrong individual or company. In particular, exercise care in using e-mail distribution lists or Networking Sites to make sure that all addressees or site group members are appropriate recipients of the information sent or posted.

Content and tone of communications

All e-mails, postings on Networking Sites and electronic communications should be courteous, professional and business-like and, as set out in sections 2 and 3, should not contain any material, which would reflect badly on the Company's reputation. If You receive an e-mail, posting or other communication containing material that is offensive or inappropriate to the office environment then You must inform [the Company's IT Manager/ your line manager/ or other] and delete on their instruction. Under no circumstances should such e-mails, postings or communications be forwarded internally or externally. [see Note 12]

Out of Office messages

If You are out of the office [for more than X hours] you should put an "Out of Office" message on your emails and on your voicemail(s). This message should indicate when you will be back in the office and should identify another person whom the sender or caller can contact in your absence should they need to.

[Your emails and phone calls [may/ will] be monitored in your absence.] [see Note 13]

Deleting or archiving material

You should not store large quantities of e-mail or downloaded files or attachments. The retention of data utilises large amounts of storage space on network servers, PCs and mobile media, and can adversely affect system performance.

You should delete any e-mails or other communications sent or received that no longer require action or are no longer relevant to Your work or to the Company.

You should retain any information that you need for record-keeping purposes in line with the Company's Information Security and Data Protection policy.

Suspect documents, messages or viruses

Any files or software downloaded from the Internet, personal mobile media or other software or hardware brought from home (and for which you have previously obtained authorisation to download as per section 2 of this policy) must be virus-checked before installation on the Facilities and use.

If you receive any suspect e-mails, communications, documents or computer virus alerts you should:

- contact [the Company's IT manager/ your line manager/ or other] immediately;
- not open attachments to any email message whose address You do not recognise; and
- not forward them to any other internal or external user without the approval of [the Company's IT Manager/ your line manager/ or other].

Passwords

Your password(s) is/ are confidential and should not be disclosed to any unauthorised person.

The Company reserves the right to access any accounts (whether email or networking sites) in which case You will be required to give Your password to [the Company's IT Manager/ your line manager/ or other].

Passwords should be changed regularly. To protect passwords, You should not access the Facilities in the presence of others and Confidential Information should never be left open on the screen when equipment is unattended.

Monitoring use of the Facilities, Professional and Social Networking Sites: [see Note 13]

The Company has the right to monitor any and all aspects of the use of the Facilities and any Networking Sites and to monitor, intercept and/or record any communications made by using the Facilities and any Networking Sites. This is to ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

By using the Facilities and any Networking Sites You consent voluntarily and knowingly to Your use being monitored. You also acknowledge the right of the Company to conduct such monitoring.

Unsolicited Communications

It is unlawful to send unsolicited emails or mobile telephone text messages to individuals with whom there is no existing customer relationship unless those individuals have given their consent.

Before any direct marketing approach is used to contact individuals by means of email or mobile telephone text message You must first obtain the authorisation of [the Company's IT Manager/ your line manager/ or other]. In any event any unsolicited communications sent in this way must include wording in the title or in the text enabling the receiver to opt-out of further contact in the future [see Note 14].

If you are using telephone or fax to contact companies and individuals with unsolicited direct marketing you must first check whether such companies or individuals are registered with the Telephone Preference Service (TPS) or Fax Preference Service (FPS) operated by the Direct Marketing Association. You may not send unsolicited direct marketing to a company that is registered with the TPS or FPS, unless you have their consent to do so.

If you are informed that an individual with whom the Company has an existing customer relationship or who has previously consented to receiving information wishes to opt-out of receiving such communications in the future you must [update the data relating to that individual immediately OR inform [Insert name of person to contact] immediately] and on no account must you continue to communicate with that individual by such means

Termination of employment or engagement with the Company

All email address lists or other contact information stored on the Facilities are Confidential Information and remain the property of the Company even after the termination of Your employment or engagement with the Company.

You may not copy or remove any email address lists or other contact information stored on the Facilities without prior written permission from the Company.

You should ensure that any genuinely Personal Contacts are, where possible, stored separately from any Professional Contacts. Upon termination of Your employment or engagement for whatever reason you may seek the Company's permission to remove or copy Your Personal Contacts from the Facilities.

On or prior to the termination of your employment or engagement with the Company for whatever reason you must speak to Your line manager to determine what steps to take in relation to any Professional Networking Sites you use. The Company reserves the right to require you to:

- advise your Professional Contacts on any Professional Networking Site of the date on which you will be leaving the Company and who Your Professional Contacts can contact at the Company when You leave the Company;
- delete Your account on any Professional Networking Site;
- delete all of Your Professional Contacts and not retain a copy of Your Professional Contacts' details without prior written permission from the Company;
- hand over control of your account on all or any Professional Networking Site(s) to [the Company's IT Manager/ Your line manager/ or other] together with all passwords. [The Company's IT Manager/ Your line manager/ or other] will be entitled to notify your contacts on all or any Professional Networking Site(s) of the fact that he/ she has taken over your account.

Employees must be aware that failure to comply with the above rules regarding Networking Sites could result in disciplinary action or dismissal even if the failure to comply occurs outside the workplace. [see Notes 8 and 11]

Status of this policy

This policy does not constitute a contract and the Company reserves the right to change its terms at any time. Failure to comply with this policy may lead to disciplinary action up to and including termination of Your employment or engagement with the Company.

Acknowledgement of receipt of policy

You are required to read a copy of this policy and return it, signed, to [your line manager/Human Resources/other] to acknowledge that you have read and understood its terms [see Note 15].

.....
Employee signature

Employee name in block capitals: