LEGAL ASPECTS OF SOCIAL MEDIA

Notes prepared for a talk to the Internet Specialist Group and the Law Specialist Group of the BCS on Monday 15 December 2014 by Jeremy Holt of Clark Holt, Commercial Solicitors

Clark Holt
COMMERCIAL SOLICITORS

HARDWICK HOUSE, PROSPECT PLACE, SWINDON, SN1 3LJ
TELEPHONE: 01793-617444 FAX: 01793-617436
WWW.CLARKHOLT.COM

Contents

Who are Clark Holt?

Clark Holt is a niche firm of commercial lawyers based in Swindon. We specialise exclusively in (1) corporate, (2) commercial and (3) commercial property law. Our website (www.clarkholt.com) provides more information about the firm. The stock in trade of the commercial department of Clark Holt is the rapid analysis (or preparation) of complex contracts. Most of our advice is given on the telephone or by email. The commercial department of Clark Holt believes passionately in plain English drafting and seeks to prepare its documents in as readable a form as possible.

Jeremy Holt is the head of the Commercial Department of Clark Holt. He founded the country's first specialist computer museum which is based in Swindon (www.museum-of-computing.org.uk). He is the co-author of "A Manager's Guide to IT Law" published by the British Computer Society (www.bcs.org/itlaw).

Jeremy Holt

Direct Dial: 01793 492256 jeremyh@clarkholt.com www.clarkholt.com

Clark Holt Commercial Solicitors, Hardwick House, Prospect Place, Swindon, Wiltshire, SN1 3LJ

This explanatory note is designed to be given to employees by their employer in order to keep them on the right track.

SOCIAL MEDIA RISKS

This business briefing highlights the risks all employees should be aware of when using e-mail and the internet at work, sending work related e-mails or discussing the workplace on the internet.

Reputational risks

What you write in e-mails or on the internet could seriously damage your own or another person's reputation, you could lose your job and you and your company could be sued, fined or even imprisoned.

Stop and think before you click

- Anything written in an e-mail has the potential for public exposure (for example, if the e-mail is forwarded to others).
- Posting on the internet is essentially making a public statement (for example, when commenting on social media sites, blogs or other electronic forums).
- Failing to take care about what you write can have serious personal, disciplinary and financial implications.
- Even if you are e-mailing or using other forms of online communication in your own time, if you refer to people at work or work related matters, you and your company could get into trouble.

E-mails and internet postings can be used in legal proceedings

- E-mails and internet postings can be used against you or your company in legal proceedings, disciplinary meetings or other regulatory investigations.
- Never delete e-mails relating to a legal dispute or investigation or potential dispute or investigation.

It is very difficult to delete e-mails and online postings

- Simply deleting e-mails or internet postings will not necessarily solve the problem. Forensic IT equipment can still find supposedly "deleted" messages.
- What you publish online will likely be available for a long time, to be read by anyone, including the company itself, future employers and colleagues.

Do not be hurtful or spread rumours

- Never send e-mails or post content online that could be thought of as obscene, racist, sexist, bullying or hurtful.

- Never lie, exaggerate or make false or inaccurate statement about another company or person. You could be sued even if an e-mail was only sent to one person.

- Forwarding an e-mail can be just as serious as writing the original – you could be sued even if the original was sent or forwarded to only one person.

Take care with confidential information

- Where possible, avoid sending confidential information (such as confidential intellectual property or trade secrets) by e-mail. Take legal advice on how the information can be best protected.

- Any e-mail containing confidential information should be clearly marked as "confidential".

- If you receive any e-mail that contains another company's confidential material (for example, a company's trade secrets) and the e-mail was not part of a legitimate transaction, you should take legal advice immediately.

Do not make a contract by mistake

- A legal binding contract can be made by simple exchange of e-mails.

- Make it clear if you do not intend the e-mail to be binding.

Do not copy someone else's work

- Only use or attach other people's work to your e-mails if you have permission or you know it is not protected by copyright or other intellectual property rights (for example, trade mark rights). This includes photographs and music.

- Do not assume that work you find on the internet is free to use.

Do not send or view offensive or unknown material

- Monitor what arrives in your inbox, especially if you do not recognise the sender or the title of the e-mail seems odd.

- If there is a risk that an e-mail contains a virus, do not open it and inform the IT department immediately.

- You could be disciplined or even dismissed for forwarding inappropriate e-mails accessing inappropriate websites at work. In severe cases it could also be a criminal offence.

Avoid unproductive usage

- Most businesses allow light personnel internet and e-mail usage as long as it does not interfere with your duties. However, excessive, unproductive usage is not permitted and may be treated as gross misconduct.

E-mails can often be a waste of time. Think carefully before copying someone in on an e-mail, especially if there is a long chain of e-mails attached.

This is a formal policy for employers to adopt in relation to their employees.

SOCIAL MEDIA AND INTERNET POLICY

1. POLICY STATEMENT

1.1 Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor their use, and the action we will take in respect of breaches of these standards.

1.2 We recognise that the internet also provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis (whether this is on our system or your personal devices and computers). We respect your right to private life, however, employees' use of social media can pose risks to our confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

1.3 To minimise these risks, to avoid loss of productivity and to ensure that IT resources and communications systems are used only for appropriate business purposes, we expect employees to adhere to this policy.

1.4 This policy does not form part of your contract of employment and it may be amended at any time.

2. WHO IS COVERED BY THE POLICY?

2. This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff (collectively referred to as **staff** in this policy).

2.1 Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

3. SCOPE AND PURPOSE OF THE POLICY

3.1 This policy deals with the use (and misuse) of computer equipment, e-mail, the internet, telephones, BlackBerries, personal digital assistants (PDAs) and voicemail. It also applies to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

3.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

3.3 It applies to the use of social media for **both business and personal purposes**, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Misuse of IT and communications systems can damage both our business and reputation. All staff must comply with this policy at all times.

3.4 Breach of this policy may result in disciplinary action up to and including dismissal and in serious cases it may be treated as gross misconduct leading to summary dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

3.5 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

4. OUR EQUIPMENT SECURITY AND PASSWORDS

4.1 Staff are responsible for the security of the equipment allocated to or used by them and provided by us, and must not allow it to be used by anyone other than in accordance with this policy.

4.2 If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

4.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting [POSITION]

4.4 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by [RELEVANT POSITION]. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to [RELEVANT POSITION] and return any equipment, key fobs or cards.

4.5 Staff who have been issued with a laptop, PDA or BlackBerry must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, other passengers on public transport.

5. OUR SYSTEMS AND DATA SECURITY

5.1 Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

5.2 Staff should not download or install software from external sources without authorisation from [POSITION]. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by [POSITION] before they are downloaded. If in doubt, staff should seek advice from [POSITION].

5.3 No device or equipment should be attached to our systems without the prior approval of the IT Department. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

5.4 We monitor all e-mails passing through our system for viruses. Workers should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .ex). [POSITION] should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this policy. We also reserve the right not to transmit any e-mail message.

5.5 Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

5.6 Staff using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by [POSITION] from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

6. OUR E-MAIL ETIQUETTE AND CONTENT

6.1 E-mail is a vital business tool, but is also an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate method for a particular communication. Correspondence with third parties by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

6.2 Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform [NAME].

6.3 Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages

may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

6.4 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

6.5 In general, staff should not:

(a) send or forward private e-mails at work which they would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

(d) sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

(e) agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;

(f) download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another worker's computer or under an assumed name unless specifically authorised; or

(h) send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

6.6 Staff who receive a wrongly-delivered e-mail should return it to the sender.

7. PERSONAL USE OF OUR SYSTEMS

7.1 We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

7.2 The following conditions must be met for personal usage to continue:

(a) use must be minimal and take place substantially out of normal working hours (that is, during the lunch hour or before or after work);

(b) use must not interfere with your work responsibilities.

8. INAPPROPRIATE USE OF OUR SYSTEMS

8.1 Misuse or excessive use or abuse of our telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be a disciplinary matter. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet on our systems by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

(e) confidential information about us or any of our staff or clients (which you do not have authority to access);

(f) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or

(g) material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

8. Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Policy. If necessary such information may be handed to the Police in connection with a criminal investigation.

9. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

9.1 Use of the internet in relation to work or the use of social media websites should never be used in a way that breaches any of our other policies. For example, employees are prohibited from using social media to:

(a) breach any obligations they may have relating to confidentiality;

(b) defame or disparage the organisation or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;

(c) post anything which could be regarded in our reasonable opinion as inappropriate or attracting unwelcome comment which affects our reputation;

(d) harass or bully other staff in any way;

(e) unlawfully discriminate against other staff or third parties;

(f) breach our Data Protection policy (for example, never disclose personal information about a colleague online);

(g) breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements);

(h) use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

9.2 Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

9. Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

10. PERSONAL USE OF SOCIAL MEDIA

10.1 We recognise that employees may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited.

11. MONITORING

11.1 The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

11.2 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications,

postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

11.3 We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

11.4 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

11.5 We may also monitor your use of the internet where information posted by you is accessible to others and it is in our interests to do so. These checks will be recorded and any information obtained will only be stored by us where it is necessary.

12. RESPONSIBLE USE

12.1 The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media and the internet responsibly and safely.

12.2 Protecting our business reputation:

(a) Staff must not post disparaging or defamatory statements about:

(i) our organisation and any members of staff;

(ii) our clients;

(iii) suppliers and vendors; and

(iv) other affiliates and stakeholders,

and staff should also avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

(b) Staff should make it clear in social media postings that they are speaking on their own behalf and refrain from identifying themselves as working for us. Write in the first person and use a personal e-mail address when communicating via social media.

(c) Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by everyone (including the organisation itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

(d) If you disclose your affiliation as an employee of our organisation, you must also 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". You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

(e) Avoid posting comments about sensitive business-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

(f) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your manager.

(g) If you see content in social media that disparages or reflects poorly on our organisation or our stakeholders, you should contact your manager. All staff are responsible for protecting our business reputation.

12.3 The contact details of business contacts made during the course of your employment are regarded as our confidential information. You may be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

12.4 Respecting colleagues, clients, partners and suppliers:

(a) Do not post anything that your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

(b) Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

13. REVIEW OF THIS POLICY

You are invited to comment on this policy and suggest ways in which it might be improved by contacting [POSITION].

NB. ENSURE THAT YOUR DISCIPLINARY PROCEDURE, EMPLOYMENT CONTRACT AND RESTRICTIVE COVENANTS ARE FURTHER UPDATED TO PROTECT YOUR BUSINESS