3.20 Communications Policy Issue 1

1. INTRODUCTION

1.1. The Company communications facilities are made available to users for the purposes of the business. Any breach of this policy may lead to disciplinary action being taken against you and serious breaches may lead to summary dismissal.

1.2. Communication plays an essential role in the conduct of our business. How you communicate with people not only reflects on you as an individual but also on us as an organization. The Company values everyone's ability to communicate with colleagues, suppliers and customers and business contacts, and invests substantially in information technology and communications systems which enable all to work more efficiently.

1.3. This policy applies to all individuals working for the Company who use the communications facilities, whether directors, departmental heads, consultants, full-time, part-time or fixed-term employees, trainees, contract staff, temporary staff, agency or home workers.

1.4. Although the detailed discussion is limited to use of email and internet facilities, the general principles underlying all parts of this policy also apply to telephone communications, fax machines, copiers and scanners. Note that some elements of personal use of communications facilities are specifically addressed at items 3.3, 4.3 to 4.5, 9.4 and 9.5, and 10.5.

2. GENERAL PRINCIPLES

2.1. You must use information technology and communications facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues and for the Company and in accordance with this policy and the other rules and procedures of the Company.

2.2. All information relating to our personnel or business operations are confidential.

2.3. Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

2.4. Particular care must be taken when using email, any company blogs or internal messaging systems as a means of communication because all expressions of fact, intention and opinion in an email may bind you and/or the Company and can be produced in court in the same way as other kinds of written statements.

2.5. The advantage of the internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter or a fax. These media should not be used to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If in doubt about a course of action, advice from a more senior member of staff should be sought

3. USE OF ELECTRONIC MAIL

3.1. Always consider if email is the best method of communication, taking into account the urgency and privacy etc.

3.2. Note that the email server adds a disclaimer notice at the foot of all mails sent, so do not seek to modify this in any way or add your own.

3.3. Except where specifically authorised by a more senior person, do not access any other person's in-box or other email folders nor send any email purporting to come from another person. If there is a practical need to using someone else's account, then by the signature, consider making this clear by signing it as follows;
"Yours sincerely/faithfully
YOURNAME
pp NAME ON EMAIL ACOUNT BEING USED"
You may also ask for the response to go direct to your normal account.

3.4. It is good practice to set email default to spell check before sending, and also to re-read and check an email before sending.

3.5. When an answer is expected from an outgoing mail, it is good practice to note the time expected for your recipient to respond eg "Please reply by the weekend".

3.6. All incoming mails should be answered in a timely manner. As a guide this is within 4 hours of receipt. If a response is not possible within the same day, or within the time requested from the sender, then it is courteous to advise the sender of the expected delay to avoid them chasing a response.

3.7. Please make sensible use of "ReplyToAll" when responding to an email as it can be a large time waster for all those having to open and read your reply when they do not need to see it."

3.8. Consider who mail are sent "To", and who is in the "Cc" and "Bcc fields as each have specific uses. The use of sending to Groups is encouraged in order to avoid situations where important mails do not get answered as the person is not at work that day.
Similarly, also avoid sending to group addresses when only a subset of people need to see the mail. Always think of the total time taken to read emails sent to groups but also balance this against the need to keep all interested parties I the loop.

3.9. Only have one person or Group address in the "To" box of an email. This is to be sure that all are clear on who is expected to answer the mail. When sending to a Group address, consider entering in the "To" box, one person in the group that you are expecting to respond, and moving the Group address to the "Cc" box. In this way it can prevent everyone in the group thinking that another member has responded.
Alternatively if you enter a Group mail address in the "To:" box, then consider addressing the body of the mail to the specific person that you expect or want to respond e.g. start the mail with "Dear XXX" or "Hi XXX"

3.10. If you receive a mail with yourself in the "Cc" box, then consider further action if you can see that the person in the "to" box is not likely to answer the mail in a timely manner e.g. if it is their day off.

3.11. Look out for mails you receive as a Blind Copy (Bcc), as to "reply to all" will give away the fact that the sender included you in the mail in confidence.

3.12. If the email message or attachment contains information which is time-critical, bear in mind that an email is not necessarily an instant communication and consider whether it is the most appropriate means of communication.

4. **Personal Use**

4.1. The Company may provide an open WIFI network as well as PC equipment specifically designated for personal use. The Company email and internet facilities are provided for the purposes of our business,

4.2. If there is use of the Company facilities for non-Company use, except those specifically outlined as for private use above, no privacy should be expected because the Company may need to monitor communications.

5. **USE OF INTERNET AND INTRANET**

5.1. Internet should be used sensibly. When visiting a website, information identifying the PC may be logged either internally or by the site visited. Therefore any activity engaged in via the internet may affect the Company.

5.2. It is discouraged from providing the Company email address when using public websites for non-business purposes.

5.3. Access to certain websites is blocked during normal working hours. If you have a particular business need to access such sites, please contact the IT department.

5.4. You must not:

5.4.1. introduce packet-sniffing or password-detecting software;

5.4.2. Use USB sticks or external storage media to transfer information from an external source to the Company network without the IT department virus scanning and approving the media first.

5.4.3. seek to gain access to restricted areas of the Company's network;

5.4.4. access or try to access data which you know or ought to know is confidential;

5.4.5. intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software; nor

5.4.6. carry out any hacking activities

5.4.7. use the Company's systems to participate in any internet chat room or post messages on any external website, including any message board or blog, unless expressly permitted in writing to do so by the Company

6. Conduct unauthorized access with intent to commit or facilitate the commission of further offences.

7. **MISUSE OF THE COMPANY'S FACILITIES AND SYSTEMS**

7.1. Misuse of the Company's facilities and systems, including its telephone, email and internet systems, in breach of this policy. In particular, viewing, accessing, transmitting, posting, downloading or uploading any of the following materials in the following ways, or using any of the Company's

facilities, will amount to gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

7.1.1. material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;

7.1.2. offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to the Company and any of its staff or its [customers/clients] or bring the reputation of the Company and any of its staff or its [customers/clients] into disrepute;

7.1.3. any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;

7.1.4. any material which, by intent or otherwise, harasses the recipient;

7.1.5. any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;

7.1.6. any material which violates the privacy of others or unfairly criticises or misrepresents others;

7.1.7. Confidential information about the Company and any of its staff, suppliers or customers.

7.1.8. any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the Company);

7.1.9. material in breach of copyright and/or other intellectual property rights;

7.1.10. online gambling; or

7.1.11. Unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

7.1.12. If the Company has evidence of the examples of misuse set out above it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

8. SYSTEM SECURITY

8.1. Security of our IT systems is of paramount importance. We owe a duty to all of our suppliers and customer to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time the system is used, all are expected to take responsibility for the security implications of what is done.

8.2. The Company’s system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

8.3. Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

8.4. System passwords should be kept safe and disclosed on a “need to know” basis. Those who have a legitimate reason to access other users' inboxes must be given permission from that other user. IT Support will provide guidance on how to do this If you have disclosed your password to anyone else (e.g. in response to a request from the IT staff) ensure that you change your password once the IT staff no longer need it. Contact IT Support for guidance on how to do this

8.5. Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner eg shredding.

8.6. You should not download or install software from external sources without having first received the necessary authorisation from the IT department.

8.7. No external device or equipment, including discs and other data storage devices, should be run on or connected to the Company's systems without the prior notification to and approval of the IT department.

8.8. You should always exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. The IT department should be informed immediately in such circumstances.

9. WORKING REMOTELY

9.1. This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment (e.g. client's equipment) whenever you are working on the Company's business away from the Company's premises.

9.2. When you are working remotely you must:

9.2.1. password protect any work which relates to the Company's business so that no other person can access your work;

9.2.2. position yourself so that your work cannot be seen by any other person;

9.2.3. take reasonable precautions to safeguard the security of our equipment, and keep your passwords secret;

9.2.4. inform the police and/or our IT department as soon as possible if either a Company laptop in your possession or any computer equipment on which you do the Company's work, even if this is personal IT equipment, has been lost or stolen; and

9.2.5. Ensure that any work which you do remotely is saved on the Company's system or is transferred to our system as soon as reasonably practicable.

9.3. Pocket computers, mobile phones and similar hand-held devices are easily lost or stolen so you must password-protect access to any such devices used by you on which is stored any personal data of which the Company is a data controller or any information relating our business, our clients or their business. This includes mobile devices such as mobile phones where company email is stored.

10. PERSONAL BLOGS AND WEBSITES

10.1. Please also see Company Social Media Policy

10.2. This part of the policy and procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

10.3. The Company recognise that in your own private time you may wish to publish content on the internet. For the avoidance of doubt, such activities are expressly prohibited during work time or using the Company's systems.

10.4. If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of the Company staff and/or you discuss your work or anything related to the Company or its business, customers or staff, the Company expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with the Company's policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for the Company.

10.5. If you already have, intend to create a personal blog or website that will say that you work for the Company, or in any way could identify you as someone who works for the Company then you should report this to your supervisor or manager

10.6. If a blog posting clearly identifies that you work for the Company and you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of the Company".

10.7. The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

10.7.1. Revealing confidential information about the Company in a personal online posting. This might include revealing information relating to the Company's clients, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.

10.7.2. Criticising or embarrassing the Company, its clients or its staff in a public forum (including any website). You should respect the corporate reputation of the Company and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance using the Company's grievance procedure.

10.8. If someone from the media or press contacts you about your online publications that relate to the Company you should talk to your supervisor or manager before responding and the Company's press office must be consulted.

10.9. Online publications which do not identify the author as a member of the Company staff and do not mention the Company and are purely concerned with personal matters will normally fall outside the scope of the Company's communications policy.

11. MONITORING OF COMMUNICATIONS BY THE COMPANY

11.1. The Company is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. the Company may monitor your business communications for reasons which include:

11.1.1. providing evidence of business transactions;

11.1.2. ensuring that Company procedures, policies and contracts with staff are adhered to;

11.1.3. complying with any legal obligations;

11.1.4. monitoring standards of service, staff performance, and for staff training;

11.1.5. preventing or detecting unauthorised use of the Company's communications systems or criminal activities; and

11.1.6. Maintaining the effective operation of the Company's communications systems.

11.2. the Company will monitor telephone, email (including content) and internet traffic data (i.e. sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of websites visited, duration of visits, and files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified at item 9.3. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using the Company's facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

11.3. Sometimes it is necessary for the Company to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with your permission.

11.4. All incoming email are scanned, using virus-checking software. AN external company may be used to undertake this scanning. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to you, the sender will automatically be notified and you will receive notice that the email is not going to be delivered to you because it may contain a virus.