Communications & Internet Use Policy

This policy sets out the Company's usage rules regarding computer, e-mail, telephone and Internet. It also sets out the Company's policy regarding monitoring of communications.

Contents

IMPORTANT

Breaches, of this policy (whether by negligence or deliberate intent) may, depending on the nature of the breach, be regarded as serious disciplinary matters which in some cases may result in dismissal.

A. **Policy Compliance**

Communication is an important part of your employment at LexisNexis UK ("the Company"). However, how you communicate with others may affect the reputation of the Company as well as you as an individual. Accordingly, you have a responsibility to use those resources in a professional, ethical and lawful manner.

This policy establishes guidelines for the proper use of our telephone and IT systems. It applies to computer use, electronic mail (e-mail), access to the Internet and telephone use.

It is important that you read and understand this policy in order to minimise the risk to yourself, your colleagues and the Company, arising from the abuse or misuse of our IT and communications systems. It is a requirement of your employment that you comply with this policy and any replacement policy, which may be introduced in the future. Failure to do so may result in disciplinary action, including dismissal. If there is anything that you do not understand, please discuss it with your manager. The Head of IT services is responsible for the management of the Company's communications systems and for ensuring compliance with this policy. The IT Department is available to give advice on any aspect of IT or telephone use.

B. **Computer Use**

Unauthorised Use

You may only make use of the Company's computer systems if you are authorised to do so by your manager. If you are given access to the Company's computer systems, you are responsible for the security of your terminal and you must not allow it to be used by any unauthorised person. Do not grant access to the Company's systems to any person unless you have express authority to do so.

You should not use the Company's computer equipment for any purpose not connected to the business of the Company unless you have express permission to do so or you are making a personal communication in accordance with paragraph F of this policy.

Access to LexisNexis Butterworths Network

As part of our membership of the Reed Elsevier network, LexisNexis Butterworths must adhere to a strict set of computer equipment access controls. These controls are put in place to reduce the risk of virus infections, hacking and other unauthorised access attempts. As a result of these rules, only authorised equipment is allowed to connect to the company network from any office location. Remote access (via Broadband / Dial up, etc) is also restricted to authorised equipment and access must only be via secure means (e.g. VPN software).

The only access allowed to unauthorised equipment (e.g. Internet café terminals) is via Citrix and VPN. Staff using unauthorised equipment may **not** access our networks directly or indirectly under any circumstances. Please contact the IT Helpdesk on 01483 257777 or ext. 7777 for further clarification on this matter.

Software

The Company licences software from a number of sources. It does not own such software and must comply with any restrictions or limitations on use of that software, in accordance with its licence agreements.

You are required to adhere to the provisions of any software license agreements to which the Company is party. Unless permitted by this policy, you should not use any software for

any purpose outside the business of the Company without the express permission of the Head of IT services. You must also comply with any other restrictions on use of software of which you are informed.

You should not copy, download or install any software without first obtaining permission from the IT Department.

Security

Where passwords are used to control entry to computer systems, networks or facilities, these must not be shared with or made available to other members of staff, or persons not employed by the Company unless expressly authorised by a senior Manager. You should not write your password down where others might have access to it.

You should change your password regularly. When choosing a password, do not choose names or words that can be easily associated with you. Access to e-mail or the Internet using another employee's user ID or password without the consent of the Head of IT services will result in disciplinary action, which could lead to summary dismissal.

Unauthorised access or modification

You are reminded that unauthorised access to computer material ("hacking"); unauthorised modification of computer material and storage of illegal information are criminal offences.

C. **E-mail use**

The Company's computer system contains an e-mail facility that is intended to promote effective communication within the organisation on matters relating to business. You should use the e-mail facilities only in accordance with this policy. In particular, you should not use the e-mail facilities for any of the purposes specified in paragraph G of this policy.

You may send personal messages by e-mail in accordance with paragraph F of this policy. Be aware that e-mail in not a secure method of communication. Personal communications should be clearly marked as such.

You should not send unsolicited commercial e-mails to persons with whom you do not have a prior relationship without the express permission of your manager.

You are reminded that messages are disclosable in any legal action commenced by or against the Company relevant to the issues set out in the e-mail. This applies to e-mail that has apparently been deleted, as copies may be stored by recipients or on back ups or may be reconstituted from disk.

The Company may monitor your use of the e-mail facilities in accordance with paragraph H of this policy.

Disclaimer

All e-mails sent from the Company should include the following wording:

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this mail in error please notify the system manager."

Sensitive information sent internally or otherwise (for example, salary spreadsheets) should be marked *"**Private and strictly confidential**".*

D. **Internet use**

If you do use the Company's equipment or network to access the Internet you should only do so in accordance with this policy. In particular, you should not use the Internet for any

of the purposes described in paragraph G of this policy ("Misuse of Communications Systems").

You may access the Internet for purposes connected with the business of the Company. Personal use of the Internet is permitted provided that it is in accordance with paragraph F & G of this policy.

Ensure that you read and comply with the terms and conditions of any Internet site that you visit. Do not download images, text or graphics, which are protected by copyright unless you intend to use these for private study or the terms of use of the site permit you to do so.

Do not download any images, text or materials, which are obscene, defamatory, racist, sexist or otherwise likely to cause offence to any person. Do not download software from the Internet without first obtaining the approval of the IT Department.

You should take extreme care in sending or inputting information to an Internet site. Never input any information which is confidential, which is likely to be defamatory or infringing of another's intellectual property or which may expose the Company to any type of legal liability. Remember that information inputted onto an Internet site is accessible by anyone, anywhere.

You must take steps to manage your own security when using the Internet. In particular, you should keep your password confidential at all times.

You should be aware that your use of the Internet may be monitored by the Company in accordance with the terms of paragraph H below.

E. **Telephone use**

The Company's telephone system is intended for business purposes. The system should be used for that purpose in accordance with this policy. In particular, you should not use the telephone facilities for any of the purposes specified in paragraph G of this policy. Personal use of the telephone facilities is permitted provided that it is in accordance with paragraph F of this policy.

You should exercise the same care when using the telephone as when using e-mail or other forms of written communication.

You should be aware that your use of the telephone facilities may be monitored by the Company in accordance with the terms of paragraph H below.

F. **Personal Use**

You may use the e-mail, Internet and telephone facilities for your own personal use, provided that this is in accordance with this policy and that your personal use:

- is kept to a minimum (both in terms of time spent and frequency);
- does not interfere with your job performance or impact on office working hours;
- does not have a negative impact on the Company either in terms of cost or reputation or otherwise; and
- is lawful.

Please bear in mind that e-mail and telephone are not necessarily secure forms of correspondence and that the Company may monitor and access records of your personal use in accordance with this policy. All personal e-mail should be clearly marked as such.

G. **Misuse of Communications Systems**

The same principles apply to your use of e-mail, telephone and the Internet as apply to any means of communication under your employment contract. Therefore, do not use e-mail, telephone or the Internet for any purposes which could be subject to disciplinary or legal action in any other context. The following are examples of misuses of e-mail, telephone or the Internet which could result in disciplinary action, including summary dismissal, being taken against you:

- Downloading, uploading, storing, sending, distributing or displaying e-mail, files or data or making any communication which:

  contain defamatory or discriminatory references or depictions of other individuals;

  contain material that is pornographic, profane or obscene, which will include not only unlawful pornographic images but also those which, whilst lawful, might reasonably be expected to be distasteful to other members of staff.

- Any communication which spreads malicious gossip about other members of staff or third parties or which amounts to abuse, discrimination or harassment on the grounds of sex, race, age or disability.

- Unauthorised copying, modification or encryption of data.

- Conducting any business, personal or otherwise, which is not the business of the Company.

- Sending, posting, or otherwise disclosing confidential information, trade secrets, or other confidential data of the Company.

- Sending chain letters, junk mail, **unauthorised** advertisements or other trivial content including jokes, quizzes and video clips.

- Sending, posting, or otherwise disclosing information directed to anyone who is not authorised to receive such information.

- Accessing or attempting to access another employee's computer, computer account, e-mail, files, or other data without the express consent of the employee or an authorised supervisor.

- Accessing or attempting to access any password-protected or restricted parts of the Company's IT systems for which you are not an authorised user.

- Downloading, copying or sending any material which is protected by copyright or other intellectual property rights belonging to a third party without their permission.

- Any use of the Company's IT or telephone systems for hacking, cracking, bugging, virus distribution, or accessing and/or tampering with systems or data without authorisation.

- Wasting computer or telephone resources or unfairly monopolising resources to the exclusion of others.

- Impersonation of a person by telephone or in an e-mail or modification of messages received.

- Use of the IT or telephone systems other than in accordance with this policy or any of the Company's other policies or procedures.

Please be aware that the following activities are criminal offences:

- unauthorised access to computer material (hacking);

- unauthorised modification of computer material; and
- Storage of illegal material.

H. **Monitoring of communications and Internet use**

All telephone, e-mail and Internet usage is logged automatically by the Company's computer system. Addressees of e-mails and Internet sites visited are logged and the content of Internet pages stored on the Company's servers. This is an automatic consequence of the way our computer system works. Except as set out in this policy, this data is not accessed or used in any way by any member of staff, other than for business continuity and IT housekeeping purposes.

The Company will monitor and keep records of your use of the e-mail, telephone and Internet access facilities for a number of reasons relevant to our business, including but not limited to:

- ensuring compliance with the terms of this policy;
- investigating breaches and potential breaches of this, and any other, Company policy;
- training and monitoring standards of service;
- accessing e-mails or voicemail messages in your absence for authorised business purposes;
- ensuring compliance with regulatory practices or procedures imposed or recommended by any regulatory body relevant to our business;
- ascertaining whether internal or external communications are relevant to the Company's business;
- preventing, investigating or detecting unauthorised use of our IT systems or criminal activities;
- maintaining the effective operation of the Company's IT systems;
- locating and retrieving lost data in the event of hardware or software failure;

We will usually confine our monitoring activities to traffic and billing data at a network level. This means that the duration and destination of outgoing telephone calls, the addresses of e-mails sent by you and the addresses of Internet sites visited by you will be routinely monitored and recorded by the Company. However, there may be occasions on which we will need to access the content of a communication sent or received by you, or monitor the content of a telephone conversation for one of the reasons set out above.

Similarly, we may monitor which Internet sites you visit and the time you spend. We may look at the content of the sites visited for one of the purposes set out above.

Unless clearly marked in the subject heading as being personal, the Company will assume that any e-mails sent using the Company's system are work-related and those e-mails (or any other form of communication using the Internet) should not be considered private. You must not designate an e-mail as "personal" when it is not, nor must you make excessive use of "personal" e-mails

The Company may remove and/or make copies from time to time of:

(i) the contents of any part of the Company's computer network, including, by way of example, email, network drives, local hard drives

(ii) the addresses of internet sites accessed by members of staff;

(iii) addresses of e-mails sent by employees.

E-mail accounts and voicemail messages may be accessed and read in an employee's absence by a member of their team or email administrator, subject to line management approval, for the purpose of checking to see whether e-mails received in their absence are work-related and require action.

Information which we obtain about your use of the Company's IT systems may be disclosed to appropriate management, personnel and, if required, to law enforcement officials.
Monitoring and logging of telephone calls, e-mail and Internet use will only take place by staff authorised by and under the supervision of the Head of IT services.

I. Data protection/privacy

Information relating to others

It is likely that during the course of your employment with the Company personal information relating to individuals will come into your possession. This could be general information, such as a person's e-mail address, or it could be more sensitive, for example in relation to an illness which has caused absence from work.

Unless this information is contained in personal communications, you should keep it confidential. Do not disclose it to any other person unless authorised to do so.

Ensure you process personal data in accordance with the Company's Privacy Policy and the Data Protection Act 1998. You should familiarise yourself with our Privacy Policy and the Act, this can be obtained from Human Resources.

Information relating to you

The Company will hold and process your personal data in accordance with our Privacy Policy.

We will retain a record of your use of the telephone, e-mail and Internet access facilities for a maximum period of 12 months. These records will be kept secure and will only be accessible by the Head of the IT Department and authorised personnel.

You are entitled to request a copy of these records. If you wish to do so please make a request in accordance with the procedure set out in our Privacy Policy. We are entitled to charge a fee for processing this request.

If you become aware that records of telephone, e-mail and Internet use by you are inaccurate, you may request that they are amended. If you wish to do so, please make a request in writing to the Data Protection Officer (whose details are set out in our Privacy Policy). If we consider the amendment unnecessary, you can add a statement to qualify or counter the records in question.

In the event that these records are used as evidence in any disciplinary action against you, you will be given a chance to explain or challenge the records.

If you have any queries in relation to your obligations or rights in relation to data protection, please contact the Data Protection Officer.

J. Laptop Users

All laptops and mobile phones users should be aware of the security risks with these items of equipment. All laptops and mobile phones, if left unattended at the office, should in every instance be locked away.

K. **Responsibilities**

It is the responsibility of each employee to adhere to this policy and to support the Company's standards.

Policy Approved by:

Name:	Mark Wilkinson
Title:	Head of IT Services
Date:	20 February 2004