



## Independent News & Media (Northern Ireland)

BELFAST TELEGRAPH • SUNDAY LIFE • COMMUNITY TELEGRAPH

A division of Independent News & Media Ltd

### "RULES GOVERNING USE OF COMPUTER SYSTEMS"

Computer systems are a vital and indispensable part of the operation of the Company. The Company's computer systems give you access to confidential and business-critical information which must be treated with the utmost care and respect. The computer systems, including network access and printers are made available to you solely for the purposes of conducting the Company's business. Without prior management written approval, they are not to be used for personal purposes.

There are a number of real threats arising from misuse and abuse of the Company's computer systems, and the rules governing computer use set out herein are designed to combat these threats. A variety of mechanisms have been put in place to help monitor the use to which the Company's computer systems are being put. A breach of any of these rules will constitute a breach of your employment contract.

#### AGREEMENTS AND COMPUTER VIRUSES

Please make sure that you:

- Use only those computer programs or computer program materials (for example, the programs themselves and user manuals) for which you know that the company has purchased licenses. If in doubt, you should obtain written clearance from the Systems Department before using programs or program material about which you are unsure.
- Do nothing in performing your duties which will result in you breaking any agreement relating to ownership of intellectual property rights or duties of confidentiality which you have, or have had, with another person or company (for example, a previous employer).
- Do not remove any computer equipment or software from the Company premises without prior written approval from the systems department.
- Do not introduce any computer software program ( for example any computer virus or software lock ) which you intend, or know is intended,
  - to impair the operation of the system or the Company's programs, or those of its clients and/or customers.

- to cause loss of, or corruption, or damage to any program or data held on the system itself.
- that you have not been given written permission to by the Systems Department.
- Limit your use of any systems to the Company's business purposes, unless you have been authorised in writing to the contrary by your Departmental manager. Do not load any personal software onto any of the Company's computer systems

### GENERAL REQUIREMENTS

You must, where applicable:

- Ensure, before you introduce any computer software, code, program or data to the system by means of, for example, a floppy diskette, CD or other electronic means, that the software, code, program or data is checked and passed for use by the Systems Department.
- Keep passwords confidential and do not reveal them to any unauthorised employee or third party;
- Use password controlled systems where they are installed and ensure that access to confidential information is controlled by a password.
- Ensure that backups of programs and data are taken at specified intervals and that one copy is stored 'off site';
- Ensure that you implement good housekeeping routines by deleting unnecessary files and data from your allocated storage areas;
- Store all diskettes and tapes in a secure environment, report any security incident to your Department Manager.
- Log off all systems at the end of your daily work schedule. If you leave your terminal unattended, you must either log off the system or have a password controlled screen saver in operation.

### PARTICULAR REQUIREMENTS

#### E-Mail/CC-Mail

Via e-mail, your computer system provides an extremely convenient means of communicating with others, both inside and outside the Company. You should not be deceived by this convenience. Messages that you send by e-mail are correspondence sent by the company.

1. You must prepare such messages using the same professional standards as you apply in preparing conventional correspondence.
2. You must not send, forward or route, either internally or externally any e-mail which is defamatory, obscene, offensive on the basis of racism, sexism, ageism, religious belief, or otherwise unlawful. You must not forward or route either internally or externally any e-mail that infringes copyright law whether belonging to the company or other companies.
3. You must not receive nor load on to the system any program, executable file, game, screen saver, video, sound file, picture or photograph unless it is accepted as part of your daily tasks and has been authorised in advance by either your Departmental Manager of the Systems Department.
4. If you regard an incoming mail as suspicious, then you must contact your Departmental Manager or the Systems Department before opening it.

#### Internet

1. Internet access is provided purely for business purposes. When using the Internet, you should be conscious of the cost effectiveness of what you are doing. Do not waste time on the Internet, and do not use it for any personal interest.
2. You must not use the Internet to access sites containing material which is defamatory, offensive, racist, sexist, obscene or otherwise unlawful.
3. You must not download anything that is not from a known and reputable web site. And you must not download any material that is defamatory, offensive, racist, sexist, obscene or unlawful. You must download or pass on anything that infringes copyright law whether belonging to the Company or other companies. You must not download any program, executable file, game, screen saver, video, sound file, picture or photograph, unless it is accepted as part of your daily tasks and has been authorised in advance by either your Departmental Manager or the Systems Department.
4. You must not set up or use any web site in advance by either Departmental Manager or the System Department.
5. You must not get involved in chats or news/user forums unless it is accepted as part of your daily tasks and has been authorised in advance by either your Departmental Manager or the Systems Department.
6. You must not divulge your Company e-mail address in any web site that is not reputable. To do so can lead to the receipt of huge volumes of unsolicited mail.

### Access Violations

1. It is not permitted to seek or gain access to any documents, data or programs that are not directly required by you for your day to day work.
2. Documents or data may not be copied from the system either by e-mail, floppy diskette, or other electronic means unless required for business purposes.
3. The software that we use is licensed. It is illegal to make copies of any software that is on the Company's computer system except for the purpose of security back-up for the company.

### Carelessness

Actions taken by you, sometimes unwittingly, can have extremely serious consequences.

1. If you don't know what you are doing, then don't do it. Ask for advice.
2. Do not delete directories or folders without explicit authorisation from the Systems Department.
3. When asked by the system "Are you sure that you want to delete...?", then be absolutely sure before you click "Yes".
4. Take appropriate care of the equipment that has been entrusted to you. It is delicate. Do not spill liquid, crumbs, paper clips or staples on your keyboard.

### Personal Use

1. You may not use the Company's computer systems for personal use unless specifically authorised in writing by your Departmental Manager.
2. It is strictly prohibited to copy data or documents to or from the computer system by floppy diskette, e-mail or other electronic media.
3. It is strictly prohibited to load on to the system using floppy disk, CD, e-mail or any other electronic media any program, executable file, game, screen saver, video, sound file, picture or photograph.
4. Only CD's required for business use should be inserted and then only with prior written approval of a Departmental Manager.

## CONFIDENTIALITY

All information contained in the Company's computer systems is confidential to the business of this Company and must be treated as such at all times by employees. In particular, details and information relating to customers is and must remain confidential and must not be passed on to any other person or any other employee, other than those employees who need to have access to such information for the purposes of performing their duties with this Company.

The only exceptions arise when information is required to be produced on foot of a Court Order or to the Police. However, such information must not be given out over the telephone and must only be released in person on production of original validating documentation including, when appropriate, Form 81.

Any breach of confidentiality will normally be regarded by the Company as gross misconduct, leading to summary dismissal.

## DISCIPLINARY OFFENCES

These Rules specify what the Company expects and requires from its employees when using the computer systems (including e-mail and internet) of the Company in the course of employment.

Employees who do not comply with these Rules or the general law regarding the use of computers (including Computer Misuse Act 1990) will face the disciplinary action up to and including summary dismissal, i.e. the immediate termination of your employment without compensation. Employees may also face prosecution for committing criminal offences, depending upon the nature of the breach committed.