ELECTRONIC AND TELEPHONE COMMUNICATIONS POLICY

Title:	Electronic and Telephone Communications Policy
Abstract:	This policy details the arrangements, responsibilities and procedures for dealing with the misuse of company electronics and telephone communications. The policy is mandatory.
Author:	*[Author Name]*
Business Approval:	*[Approver Name]*
Date Issued:	*[Date Issued]*

AMENDMENT RECORD

Issue Number	Date Issued	Description and Author
001		Original Issue

Electronic and Telephone Communications Policy

Computer Misuse

Many employees have access to computers at work for use in connection with Company business. Employees who are discovered unreasonably using the Company computers for personal and private purposes will be dealt with under the Company disciplinary procedure.

Vandalism of, or otherwise intentionally interfering with, the Company's computer network constitutes a gross misconduct offence and could render the employee liable to summary dismissal under the Company's disciplinary procedure.

Email and the Internet

Many employees have access to email and the Internet for exclusive use in connection with the Company's business and as part of the normal execution of their job duties. The purpose of these rules is to protect the Company's legal interests. Unregulated access increases the risk of Employees inadvertently forming contracts through email and increases the opportunity for wrongful disclosure of confidential information. In addition, carelessly worded email can expose the Company to an action for libel. As such, email to clients and customers must follow the Company's designated house style, which will be supplied to authorised users. Failure to follow house style is a disciplinary matter and will be dealt with under the Company's disciplinary procedure.

Email should not be used for unsolicited correspondence or marketing campaigns and Employees may not commit the Company financially by email unless they have been granted a specific level of delegated authority to do so.

Employees who are authorised users are not permitted to surf the Internet or to spend excessive time "chatting" by email or any other communications channel for personal and private purposes during their normal working hours. The use of instant messaging systems is expressly prohibited at work unless for communications with customers. Employees are also prohibited from using email to circulate any non-business material.

Excessive time spent online lead to loss of productivity and constitute an unauthorised use of the Company's time. Also sexist, racist or other offensive remarks or jokes sent by email are capable of amounting to unlawful harassment. Employees who are discovered contravening these rules may face serious disciplinary action under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or obscene material or using the Internet for gambling or any illegal activities constitutes gross misconduct and could render the employee liable to summary dismissal under the Company's disciplinary procedure.

The Company reserves the right to monitor Employees emails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are:

- To promote productivity and efficiency.
- For security reasons.

- To ensure there is no unauthorised use of the Company's time e.g. that an employee has not been using email to send or receive an excessive number of personal communications.
- To ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked.
- To ensure that all employees are treated with respect, by discovering and eliminating any material that is capable of amounting to unlawful harassment.

Communications of a sensitive or confidential nature should not be sent by email because it is not guaranteed to be private. When monitoring emails, the Company will, save in exceptional circumstances, confine itself to looking at the address and heading of the emails. However, where circumstances warrant it, the Company may open emails and access the content. In this case, the Company will avoid, if possible, opening emails clearly marked as private or personal.

The Company reserves the right to deny or remove email or Internet access from any employee.

Use of Email Summary

1. No communication may contain any references to other individuals which might be construed as libellous.
2. No communication which might be regarded as harassing or insulting may be sent using the Company's system. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis as is normal courteous practice.
3. The company recognises that it is not always possible to control incoming mail. Any material which would be considered as non-business-like, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communication from known sources is responsible for contacting that source in order to request that such communication is stopped.
4. If members of staff receive virus warnings via email, they should take no action whatsoever other than informing the IT staff immediately.
5. Emails sent internally may be sent in an informal style, but staff are asked to observe the normal courtesy that they would extend in written memos as per the house style.
6. Emails which are sent to recipients outside the Company should be composed in a business-like manner. A guideline for suitable styles is available and this should be followed at all times. Any attachments such as letters must be headed and written accordingly to the normal house style.
7. Unsolicited Emails may not be sent at any time. Any "junk" mail received should be deleted immediately.
8. All attachments received within an email must be checked for viruses.
9. The email address book will be maintained by IT staff to whom any changes should be advised. Company Email addresses for all Employees will be issued by IT staff and may not be changed without their authorisation.
10. it is a disciplinary offence to access another individual's email account by using their password without their express permission.

Computer Software Games and Malware

The Company licences the use of computer software from a variety of outside sources. The Company does not own this software and, unless authorised by the software developer, neither the Company nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Contravention is a disciplinary matter and will be dealt with in accordance with the Company's disciplinary procedure.

Computer networks are always vulnerable to malware. Therefore, only duly authorised personnel have the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for malware by authorised personnel. Any employee found to be contravening this will face disciplinary action under the Company's disciplinary procedure.

Employees may only access any computer games that are on the network outside their normal working hours.

Telephone Misuse

The Company's telephone lines are for the exclusive use by employees in connection with the Company's business. Whilst the Company will accept the need for essential personal telephone calls concerning an employee's domestic arrangements, excessive use of the telephone for personal calls is prohibited. This includes lengthy, casual chats and calls at premium rates. Not only does excessive time on personal telephone calls lead to loss of productivity, it also constitutes an unauthorised use of the Company time and resources. If the Company discovers that the telephone has been used excessively for personal calls, this will be dealt with under the Company's disciplinary procedure and the employee will be required to pay to the Company the cost of personal calls made.

Acceptable telephone use should be no more thana few minutes of personal calls in each working day. Personal telephone calls should be timed so as to cause minimum disruption to the Employee's work and should only be made during breaks except in the case of a genuine emergency.

Employees should be aware that telephone calls made and received on the Company's telephone network will routinely be monitored and recorded to assess employee performance, to ensure customer satisfaction and to check that the use of the telephone system is not being abused.