SYFA Limited (SYFA)

ITC, EMAIL & INTERNET POLICY

ITC, EMAIL and INTERNET POLICY

1. Introduction

1.1 SYFA Limited ("SYFA") wishes to assure, as practically as possible, the integrity and security of its networks, data and applications. To achieve this requirement users must access the system in an acceptable manner which includes the requirement for each director and employee to have completed and signed a declaration to verify his/her reading and understanding of this Policy. For details of the SYFA declaration refer to Appendix 2.

1.2 Employees are responsible as computer users to ensure that they show good working practices when using the IT equipment and do not compromise SYFA either morally or legally.

1.3 Employees should be aware that a breach of this Policy could be viewed as gross misconduct and will entitle SYFA to take disciplinary action against the relevant member of staff in accordance with the disciplinary procedures.

1.4 This policy provides some guidance on what your responsibilities are and processes SYFA undertakes on your behalf to protect you. Companies who do not comply with the legal guidelines set down for computer use leave themselves vulnerable to an unlimited fine or imprisonment. It is vital that we all work together to ensure compliance.

2. Purpose

The purpose of this document is to ensure that all individuals are aware of the general principles and rules surrounding the acceptable use of SYFA's information system. It also explains how the SYFA monitors systems use and its response to inappropriate/forbidden use. For details of Inappropriate/Forbidden use refer to Appendix 1.

3. Scope

3.1 SYFA is heavily dependent on the computer systems and the information that they generate to achieve its aims and objectives.

3.2 All individuals (directors, employees and volunteers) who use or have access to the SYFA's information systems are covered by this policy and should be familiar with its content. No provision is made for visitors. It covers office based computers and laptops which may be used inside or outside the office.

3.3 Failure to comply with the policy or deliberate misuse, negligence of abuse of the firm's systems, equipment and electronic services may result in disciplinary action up to and including summary dismissal.

3.4 This policy is reviewed and updated periodically.

4. Security - General

4.1 Keep equipment and data safe:

4.1.1 Computer equipment and data should only be used for authorised purposes;

4.1.2 If you are connected to the network store all files on the server (no files should be stored on your desktop) to ensure that they are included within the regular back up;

4.1.3 If you are not connected to the network you are obliged to take separate measures to back up your data on a regular basis;

4.1.4 Store discs and back-up tapes securely. If they contain confidential data, lock them in a fireproof safe or cabinet or remove to another location;

4.1.5 Files, discs and software should be checked for viruses prior to installation;

4.1.6 Dispose of 'Confidential Waste' securely.

4.2 Security of IT equipment outwith the SYFA's premises:

4.2.1 Portable computer equipment is a valuable and vulnerable commodity. Make sure you look after it!;

4.2.2 Use of SYFA's computer equipment or data outwith the premises must be authorised;

4.2.3 Common sense should be applied at all times. Do not, for example, leave a laptop unattended or visible in a car;

4.2.4 Staff travelling outwith the UK should inform the National Secretary as it may be necessary to increase SYFA's insurance protection.

5. Software

5.1 Software Integrity

5.1.1 Do not make non-licensed copies of software on the network;

5.1.2 Unauthorised games or screensavers are not permitted on equipment.

5.2 Software Acquisitions and Disposal

5.2.1 To comply with software licenses and to ensure that only standard software is deployed SYFA has introduced the following policy for software acquisition;

5.2.2 Staff should be aware that contradiction of this policy could lead to disciplinary measures;

5.2.3 Software disposal will be undertaken by SYFA. Staff are discouraged from deleting software programmes themselves. You should notify the National Secretary who will arrange the proper deletion of software;

5.2.4 Any member of staff who carries out this procedure themselves and causes software errors will be liable to disciplinary action.

6. Viruses – What to do to protect Data & Software against Viruses

6.1 Viruses are a major threat to the integrity of the SYFA's computer system and are easier to prevent than to remedy. Following the guidelines below should prevent the introduction of any malicious code:

6.1.1 Never load unauthorised software onto your computer;

6.1.2 Antivirus software is updated on the network on a regular basis;

6.1.3 Report any suspicions of virus infection to the National Secretary immediately;

6.1.4 All discs, CDs and other transportable media must be virus checked prior to use on the SYFA's equipment.

7. Internet

7.1 SYFA may decide at its discretion which members of staff may have Internet access from time to time and to what extent and any permission given to a particular employee may subsequently be withdrawn.

7.2 Do not enter your e-mail address on a website unnecessarily. If you give your address when filling in surveys or other questionnaires you will be at risk of receiving unwanted junk messages.

7.3 Personal use of the internet is permitted as a privilege and only on the following conditions:

- 7.3.1 The personal use must not be in breach of this Policy;
- 7.3.2 The personal use must not be excessive;
- 7.3.3 The personal use must not interfere with business or office commitments;
- 7.3.4 The personal use must take place outside working time, in the User's own time (before the office opens for business, at lunch time, or after the office is closed);
- 7.3.5 The SYFA is not responsible for any loss of confidential information divulged by the employee (for example their credit card or bank details);
- 7.3.6 The User acknowledges that the security of the System is devised with a view to its use for the SYFA's business, not for private use; and
- 7.3.7 No liability of any kind is to attach to the SYFA, attributable to or arising out of the User's personal use.

7.4 The SYFA reserves the right to restrict or prevent access to certain telephone numbers, email addresses or internet sites if it considers that personal use is excessive.

7.5 You should be aware that any personal use of the Systems may also be monitored in accordance with this Policy.

8. Social Media

8.1 Internet provides a number of benefits in which staff may wish to participate. From rediscovering old school friends on Facebook or Friends Reunited or helping to maintain open access online encyclopaedias such as Wikipedia.

8.2 However, when someone clearly identifies their association with SYFA and/or discusses their work, they are expected to behave appropriately when on the Internet and in ways that are consistent with the SYFA's values and operational policies.

8.3 As part of the SYFA strategy and to keep up to date with both technology and networking you are actively encouraged to make use of social media sites such as Twitter, LinkedIn and professional blogging sites to promote the SYFA and its services.

8.4 LinkedIn accounts

- 8.4.1 Whilst these accounts are primarily used as a professional tool they are neither private nor public however there are a number of sensible steps that employees must adhere to;
- 8.4.2 Should you resign or be dismissed from SYFA by whatever reason you will be required to update your employment status immediately upon termination.

8.5 Facebook accounts

8.5.1 You are not permitted to use your personal Facebook account during work nor be deemed to be representing SYFA. Whilst Facebook is used in your own time, and is a personal social networking tool employees must be aware that damaging the SYFA's reputation or putting SYFA into disrepute on your Facebook / bebo / myspace / twitter/ or any other account will be dealt with under the SYFA disciplinary policy. Employees should be mindful of the information that is posted on their own social networking sites.

8.5.2 For example if you are on a work night out or there are photographs of you with another colleague from the SYFA, you are mindful of their privacy and the reputation of the SYFA. Under no circumstances should there be offensive remarks about any colleagues on any social media or networking sites.

8.6 Blogging

8.6.1 Whilst you are being encouraged to share SYFA updates and industry news with social media users you may also be privy to information that is sensitive and that others in SYFA are not therefore you must use complete discretion in the information that you post to avoid breach of confidentiality on business or in fact clients and employees.

8.6.2 Where you are blogging at home, not identified as an employee of the SYFA and do not discuss the SYFA and it is purely on personal matters, would fall outwith the remit of this policy. Should you indicate that you are an employee of the SYFA you should make clear that these are your personal views and not those of the SYFA.

9. Electronic Mail (E-Mails)

9.1 SYFA is committed to the widespread use of electronic mail (e-mail) in order to improve efficiency and productivity and to save on paper.

9.2 E-mail is a valuable addition to the more traditional means of communication. It is fast and the sender can receive confirmation of when the recipients received and opened the message. Text can have files attached and can be copied to several people without the need for photocopying and postage. The potential for improved speed and efficiency is great.

9.3 Inappropriate use, however, causes many problems ranging from minor distractions, system corruptions and information overload to legal claims against SYFA and individual employees.

9.4 All e-mail data stored on the SYFA's servers from time to time is the property of SYFA and SYFA can deal with such data in whatever manner it may decide.

9.5 Content and Style:

9.5.1 E-mail is associated with the 'popular' culture of the internet and, stylistically, can seem closer to speech than a written fax or memo. Users sometimes, therefore, view e-mail as an informal means of communication;

9.5.2 In fact it is nothing of the sort. There is a permanent written record of each e-mail message and these are considered as standard evidence in legal disputes.

Each e-mail message should be written and checked with the care given to a formal letter on the firm's letterhead. Each comment passed to colleagues or staff should be considered with the caution and foresight that would be used in a formal setting;

9.5.3 Each message should always include a clear subject heading which is as short and meaningful as possible. E-mails received that do not have a subject must not be opened and must be deleted;

9.5.4 In the body of the message try to keep to the point and keep the message short. If you need to move onto another topic you should consider sending another message;

9.5.5 Use e-mail with attachments wherever possible and appropriate. It cuts down on paper and saves time and photocopying costs. Do not however use an attachment where the text or the attachment is just as easily typed into e-mail. Attachments should not be larger than 100kb in size. (You can find the size by clicking onto "file" and then "properties");

9.5.6 The SYFA's usual standards for written correspondence apply to e-mail, both in respect of language and grammar and for consideration of people;

9.5.7 The laws of defamation, copyright and decency apply to e-mail. Users must not send text or images which contain anything that may bring the SYFA into disrepute. Information which could be regarded as sensitive or confidential should not be transmitted via e-mail;

9.5.8 Typing text, other than headings, in upper case is the re-mail equivalent of SHOUTING. This may be interpreted as harassment and/or bullying. Shouting via e-mail is no more acceptable than it is face to face and should be avoided;

9.5.9 Consider the appropriateness of using e-mail. It should not be used as a substitute for face to face communication or for using the telephone. "Flame mails" (e-mails that are abusive) can be a source of stress and damage work relationships;

9.5.10 If you are communicating the SYFA's policy or representing SYFA's views first ensure that you have the authority to do so;

9.5.11 Pay careful attention to whom you send the message and ensure it is properly addressed. Consider carefully the extent of circulation and send a copy message only to those for whom it is particularly relevant.

9.6 Responding

9.6.1 Never respond to any e-mail that does not have a subject. These e-mails must be deleted;

9.6.2 When replying to a message, include the original message to provide a context;

9.6.3 Respond promptly to e-mail sent to you. Establish a daily routine for your e-mail;

9.6.4 When copying or forwarding messages take care to respect the original sender's intent;

9.6.5 Avoid arbitrarily passing messages intended for one person on to others;

9.6.6 Only copy e-mail to necessary recipients and avoid unnecessary distribution.

9.7 Standards to uphold when using e-mail

9.7.1 Do not use e-mail for political or commercial reasons. It should generally be used for business purposes only;

9.7.2 Report any suspicions of virus infection to the National Secretary immediately;

9.7.3 Do notify the National Secretary immediately if you receive e-mail that is inappropriate or offensive.

9.8 Personal E-mails and Monitoring

9.8.1 As stated above, SYFA recognises that some personal use of SYFA's e-mail system is permissible. This must be kept to a reasonable level and you should not enter into extensive e-mail correspondence on a personal basis;

9.8.2 SYFA may engage in the monitoring of electronic mail messages or other electronic files created by staff for valid business purposes, including employee supervision. SYFA may also monitor any e-mail messages or other electronic files created by employees for personal purposes;

9.8.3 Employees should recognise that they do not have an expectation of privacy in relation to personal e-mails. To limit the likelihood of personal e-mail content being read you should include the word 'personal' in the subject line of the e-mail and encourage contacts to do likewise.

9.9 Housekeeping

9.9.1 Storing large amounts or work in the Inbox and Sent Items folder can slow down and reduce the capacity of your PC and can cause other technical difficulties. You should regularly clear out your e-mail by deleting unwanted messages and moving old but required messages to a separate folder or drive. The firm will regularly monitor to ensure this is being done;

9.9.2 For planned absences engage the "Out of Office Assistant" which will alert those sending messages to you of your absence and when you will return. This can be found in the drop down menu after clicking on "Tools".

9.10 Printing and Record Keeping

9.10.1 Avoid routinely printing e-mail;

9.10.2 If a message needs to be stored for a temporary period save it to hard disk;

9.10.3 You should however print off and file any e-mail communications that may later be needed as proof of that exchange.

9.11 E-mail Security

9.11.1 E-mail is neither a private or particularly secure method of communication. Outgoing messages may end up going to someone other than the recipient. This is particularly relevant when sending messages beyond the SYFA;

9.11.2 All e-mail and internet messages, text and images sent, received, downloaded or stored on the firm's system are the property of the SYFA. They can be inspected at any time and will be monitored to ensure compliance of this policy;

9.11.3 Messages, images and text are stored on the SYFA's system for up to two years, even though the user may have deleted them from his/her screen;

9.11.4 Certain types of files e.g. exe.jpg and bmp, amongst others may be intercepted by the SYFA and routed to the IT Department. These are generally the types of files that carry animation, pictures and games;

9.11.5 They are also the bigger files and the ones that are the common carrier of viruses. The SYFA will be able to monitor where these files are being sent from and to whom. If necessary in order to protect the SYFA's systems and prevent abuse, SYFA may notify the employers of the sender, informing them of the nature of the files being sent.

9.12 Harassment and Bullying

Sexual, racial and disability harassment and/or bullying carried out by e-mail is no less offensive to the recipient and no more tolerable to the SYFA than face to face contact.

9.13 Policies and Legal Issues

9.13.1 SYFA's policies regarding equal opportunities, discrimination and harassment apply to e-mail just as they do to every other aspect of working life;

9.13.2 E-mail is also subject to national law, in particular the Computer Misuse Act, Copyright Act, Data Protection Act and the law of libel;

9.13.3 The fact that e-mails can so easily and quickly be forwarded to others and that e-mails are not automatically and permanently deleted when wiped from a desktop means that defamation is a real danger. Care should be taken with the content of messages and derogatory remarks about another employee, director, SYFA member, individual person or company should not be made;

9.13.4 The same rule applies to indecent, sexist, racist or obscene remarks.

10. Passwords

10.1 Passwords will be recorded by the National Secretary for emergency use.

10.2 Do not write your password down. Commit it to memory.

10.3 Colleague's passwords should never be used to gain entry to their computer, except in their absence where work is required.

10.4 If your password is compromised, report the matter immediately to the National Secretary.

APPENDIX 1

FORBIDDEN USES

Users are forbidden to use the Systems to do any of the following:

- Cause or permit junk mail from sites to be sent to them
- Send or forward private e-mails at work which the User would not want a third party to read
- Open any e-mails, email attachments or download anything not from a trusted source
- Access on-line auction sites for personal use (for example “e-Bay”)
- Access and/or post messages to on-line chat rooms or message boards unless otherwise permitted by the SYFA to do so
- Create or contribute to an on-line diary or “blog”, even in the User’s own time unless otherwise permitted by the SYFA to do so
- View or create or send or forward illegal material
- Create or send defamatory material
- Transmit confidential information or operational secrets of the SYFA or its members and contacts, other than in the legitimate course of business
- View or create or send or forward pornographic or sexually explicit material
- View or create or send or forward material that may cause offence to others, including, but not limited to discriminatory material or material that would violate the dignity of others or create an offensive or degrading environment at work (whether or not that is intended) including on the grounds of sex, race (including ethnic or national origin), religion or belief, sexual orientation, disability or age
- Download, store or reproduce copyright material (in the UK, just about anything has copyright in some aspect) including music and video files without authorisation from the right’s holder
- Subscribe to any free e-mail services not related to the business of the SYFA using your SYFA email address
- Post or register a SYFA e-mail address on external websites or bulletin boards for personal use
- Forward any chain e-mail message (one that contains a forwarding request to be repeated in what is forwarded)
- On-line gambling
- Anything likely to harm the commercial interest, reputation or objectives of the SYFA
- Anything harmful to the Systems
- Anything for a business purpose that is not of the SYFA.

APPENDIX 2

DECLARATION

I have read the SYFA Limited's policy of acceptable use of the IT systems and acknowledge that failure to comply with the rules contained in this document may result in restriction/suspension of the use of the IT systems.

Also any inappropriate or unauthorised use of the internet or e-mail facility is likely to result in disciplinary action including summary dismissal.

I accept that the company also retains the right to report any illegal violations to the appropriate authorities.

Signature: ……

Print name ……

Date ……