Your fastest way to learn. Why wait?

FIREBRAND

Group IT Policy

August 2018

GROUP IT POLICY

POLICY OVERVIEW

The use of the E-mail system and the Internet within Firebrand is actively encouraged, given that appropriate usage facilitates timely communication and improves the efficiency and effectiveness of our employees at all levels. Used correctly, both are facilities that may improve our relationships with our clients and demonstrate that we are part of a progressive organisation.

However, the inappropriate usage of either facility may cause problems that may range from minor distractions to loss of business or even legal claims against the company. This policy therefore sets out our current thinking on the correct use of our systems as well as our policy in dealing with misuse.

The policy may change from time to time in the light of updated legislation and the ever-developing case law covering these areas.

1. Information Technology Management

Management is responsible for providing the necessary skilled personnel and resources to ensure the effective and efficient IT infrastructure to support our core Business processes.

The Head of IT has overall responsibility for the IT systems and products, in accordance with the company's portfolio.

1.1 Conditions of Use

The E-mail system and the Internet are available for communication on matters directly concerned with the business of the company. Users of the E-mail system should give particular attention to the following points:

1.1.1 Presentation

All employees should observe the standards that are reasonably expected from the company in relation to all written communications. Internal guidelines will be issued from time to time, but if in doubt, please refer to your immediate manager.

1.1.2 Circulation

E-mails are only to be sent to your colleagues for whom the message is relevant. A culture in which everyone is copied in on unsolicited messages is to be avoided if we are all to work efficiently and effectively.

1.1.3 Appropriateness

When sending a communication by E-mail to either an internal or external recipient, you should consider its appropriateness as a medium for the communication. E-mails should not be used as a substitute for face-to-face communication.

1.1.4 Content

You should carefully consider the wording in the content of all E-mails. In particular, the following rules are to be observed:

- "Flame Mails" (E-mails that are abusive) can be a source of great stress to colleagues and may damage working relationships.
- Hasty messages that are sent without due care and attention may be the source of misunderstandings, so please consider how the recipient of your E-mail may actually interpret your message.

1.1.5 Visibility

If the nature of your message is confidential, you must ensure that all necessary steps are taken in order to maintain confidentiality, thereby protecting the interests of the company. The company may also be liable for any defamatory information or comment that is passed to either internal or external users of the system.

1.1.6 Contracts

The use of E-mail has become an acceptable tool for communication in recent times. In addition to the Civil Evidence Act, 1995, which allows for E-mail to be used as evidence in the event of a dispute, recent case law has proclaimed that any offer or contract that is transmitted by E-mail is likely to be as legally binding on the company as those that are sent on paper. As a result, the company reserves the right to hold an employee accountable for their actions.

1.2 Non-Authorised Use

Firebrand will not tolerate the use of the system for any of the following:

- Transmitting or inviting any material which may reasonably be described as:
  - Unlawful;
  - Threatening;
  - Abusive;
  - Libellous;
  - Hateful;
- Breaching the Social Media policy
- Encouraging conduct that would constitute a criminal offence.
- Any message that constitutes, or could reasonably constitute, bullying and/or harassment, be it on the grounds of:
  - Age;

    - Disability;
    - Gender;
    - Gender re-assignment;
    - Marriage or civil partnership;
    - Race or ethnic origin;
    - Religion or belief;
    - Sexual orientation; or
    - Any other form of bullying and/or harassment.
- Excessive personal use, including, but not restricted to:
    - Chain letters;
    - Sale or goods.
- Accessing/downloading pornography or any other material that could reasonably be construed as being offensive.
- Accessing chat rooms.
- On-line gambling.
- Downloading or distributing copyright information and/or any software available to the user.
- Using and/or downloading games.
- Hacking (i.e. attempting to access the accounts of others, or attempting to penetrate the system security measures of the company, or any other organisation).
- Posting confidential information relating to:
    - The company; or
    - Its employees; or
    - Its customers; or
    - Its suppliers.

1.3 Copyright

Copyright includes, but is not restricted to:

- Software;
- Images;
- Photographs;
- Fonts;
- Sounds;
- Music; and
- Logos

Breaching copyright is a criminal offence as well as being a civil wrong and, unless otherwise stated, all materials on the Internet or sent by E-mail should be considered as copyrighted work and cannot therefore be downloaded, forwarded and/or modified without the permission of the copyright holder. In addition, any such files of software may only be used in ways that are consistent with their licences or copyrights. For example, prior to making a presentation to a (potential) client, you should ensure that permission is received to use company logo in the presentation.

1.4 Security

1.4.1 Downloading

Software Files
Software files from the Internet or which have been received by E-mail from an external source should not be downloaded without the express permission of the IT Manager.

On-Line Audio Visual
This represents significant data traffic, which may cause congestion. Use of this is therefore prohibited, other than for agreed business purposes.

Virus Detection
All downloaded files must be scanned with virus detection software before installation or execution.

1.4.2 Viruses and Tampering

The introduction of viruses or maliciously tampering with the IT system is strictly prohibited.

1.4.3 Confidential Information

If the content of any E-mail could reasonably be described as being confidential, then you must consider what action needs to be taken in order to maintain such confidentiality. This may include:

- Password protecting the document; or
- Using another medium.

1.4.4 Critical Information

Critical information should not be stored solely on the E-mail system. Hard copies or backup copies must be kept elsewhere in the IT system (i.e. Shared Drive, Onedrive etc).

Again, you should consider password protecting and encrypting such documents.

1.4.5 Disclaimer

The company's standard disclaimer should be used on all E-mail communications.

1.4.6 Data Protection and GDPR

You are required to be familiar with the requirements of the Data Protection Act, 1998 and to ensure that you operate in accordance with its requirements.

Firebrand will comply with the Code of Practice as issued by the Data Protection Commissioner, current from time to time.

Firebrand takes the security and protection of personal data very seriously. We are committed to providing a compliant approach to data protection. We have always had a robust data protection program in place which complies with existing law and abides by the data protection principles and we have reviewed this program to ensure that it will meet the requirements of the EU General Data Protection Regulation ("GDPR") which comes into force on 25 May 2018. When we process any personal data, we will do so according to the data processing principles of the GDPR

Reference to the full Privacy Policy is available on the public website (http://www.firebrandtraining.co.uk/privacy-policy)

1.4.7 Monitoring

There may be occasions when the company is reasonably required to access and record any communication. As we do not wish to contravene your right to privacy, we will only undertake such action without your consent, in order to combat crime or unauthorised use.

Whilst the company may introduce blocking tools in order to prevent visits to unsuitable sites, with the ever-changing nature of the Internet it is not possible to block all such sites. If you accidentally connect to a site that contains inappropriate content, you must disconnect from the site immediately and advise your immediate manager. The company has monitoring software in place and any excessive usage will be highlighted in reports and management alerted as necessary.

The company will comply with the Code of Practice as issued by the Data Protection Commissioner, current from time to time.

Retention policies are enabled reduce the liabilities associated with email and other communications. With these policies, Firebrand can apply retention settings to specific folders in users' inboxes. Administrators can also give users a menu of retention.

1.5 Training

IT training will be provided at various stages of your employment with the company. Team leaders are required to ensure that their team members attend relative training prior to using the E-mail and Internet systems and that appropriate training needs are addressed on a timely basis thereafter.

1.6 Disciplinary Procedure

You should be aware that failure to comply with these guidelines could result in the disciplinary procedure being invoked against you. In the event of a serious breach of policy, then this may even result in summary dismissal.

Please refer to the Disciplinary & Appeals Procedure for further guidance.

1.7 IT Related Health and Safety Issues, Including Workstation Guidance

The use of Information Technology has increased substantially during recent years. As a result, the responsibilities of Firebrand as an employer have changed, particularly in relation to the following:

1.7.1 Eye Sight Testing *(applicable to UK based employees only)*

If you regularly use Display Screen Equipment (e.g. VDUs) for more than one hour continuously per day, you are entitled to claim reimbursement of the following expenses:

- The cost of annual eye tests (more frequently if there is a reasonable requirement); and
- The cost of basic corrective equipment (this includes basic frames and lenses) up to a value of £75.

You are required to cover any additional cost incurred in relation to items such as designer frames, special lenses, contact lenses, etc.

1.7.2 Repetitive Strain Injury (RSI) and Work Related Upper Limb Disorder (WRULD)

Both of these conditions can occasionally be caused by:

- Performing certain tasks on a constant basis and with little or no interruption or rest; or
- Undertaking duties in a manner that is known cause damage or injury to the upper limbs.
- Examples of the above may include the incorrect use of a keyboard, poor posture (which can arise through working with inappropriate or out-dated equipment and other office furniture) and inadequate interruptions to repetitive work or rest breaks being taken.

Whilst the company will take every reasonable precaution to minimise the risk of RSI and WRULD, all employees have a responsibility to adopt good working practices and to take the advice that arises from an assessment of their work-station. If you are concerned that your workstation is not ergonomically correct or if you begin to experience symptoms of either condition, then you should raise the matter with your immediate line manager.

Medical opinion continues to develop, as the world of work becomes more familiar with advanced technology and associated disorders. Up to date advice leaflets are available from management.

1.8 Complaints

If you feel that you have cause for complaint as a result of E-mail communication or Internet activity, then you should raise the issue with your immediate manager in the first instance.

If necessary, you may have recourse to the Grievance Procedure.

NOTE: Where the above document refers to specific acts of legislation, these are UK law specific, but it should be assumed that the equivalent local act/law would apply where it exists. If not, then the intent from the company's purposes under UK law should be assumed to apply to local regions.

2. Cybersecurity and Password Policy

The intention of this policy is to protect Firebrand's network infrastructure and information systems from uncontrolled or unauthorised access which may result in Intellectual Property loss or data destruction. All users have a responsibility to ensure that they act in a way that protects unauthorised access to Firebrand's systems and data.

2.1 General Password Guidelines

Passwords should contain the following characteristics:

- At least eight characters;
- Both upper and lower case characters;
- At least one digit and one punctuation character.

Passwords must not:

- Be found in a dictionary, or be a common use slang word;
- Be a computer term, name, program, site, company name etc.
- Contain the words "password" or any derivation;
- Contain birthdays, phone numbers or other personal information;
- Use word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
- Use any of the above spelt backwards;
- Use any of the above preceded or followed by a digit (e.g. secret1, 1secret).

Passwords must be changed from their initial default value the first time a new user logs in, and at least every six months thereafter.

Passwords should never be sent via email or other forms of electronic communication.

A strong password should not be easy to guess, but it should be easy to remember, to prevent the necessity for the password to be written down. One way to do this is create a password based on a phrase or saying. For example, the phrase might be: "As sick as a dog" and the password could be "A5!kaD0g.

- A password that is used elsewhere (e.g. home internet, hotmail, etc.) should not be used as a Firebrand password.
- Passwords, or even the format of passwords, should not be shared with anyone. You are responsible for the integrity and security of your password and you are therefore liable for any misuse of the password.
- The "Remember Password" feature of applications (e.g. Outlook) should not be used.
- Passwords should not be written down, or stored on any computer (including laptops and PDAs).
  Passwords should be changed immediately if it is suspected that they have become known by another person.
- Passwords may be checked automatically to ensure they are sufficiently complex. Routine password auditing may be performed by Firebrand to ensure compliance with these standards.
- Password security is your personal responsibility and a failure to comply with this policy may result in disciplinary action.

2.2 Additional Cybersecurity Guidelines

Users must ensure that they avoid:

- Connecting to the internet over unsecured connections
- Opening emails/attachments from suspicious or unverified sources.
- Working in Physical locations e.g. cafes/public transport where confidential information may not be securely protected
- Leaving screens unlocked when absent from desk
- Tampering with any anti-virus software installed on company IT equipment.

3. Asset management

Firebrand Trainings assets include:

- IT Systems
- Laptops and Desktop PCs
- Telephone Consoles and Headsets
- Company Mobile Phones and Smart Phones
- Information

All physical assets must be uniquely labelled and recorded on the asset register – Hardcat, recording: Makes, models, Serial Numbers, Owners and Locations. Portable assets (laptops, mobile phones etc) allocated to individual users will also be recorded in the Octopus HR system by the MIS team.

Allocated owners are responsible for ongoing maintenance and security of the assets, and reporting any theft, loss or suspected compromise to line management and the MIS team in a timely manner. Any compromise of assets (deliberate or accidental) may be treated as misconduct (including gross misconduct) and dealt with under the company's disciplinary process.

All assets must be used for official company business and assets may only be removed from the premises with permission from line management and the Head of IT. Use of assets must comply with the acceptable use policies in section 1 of this policy.

4. VPN Access

The purpose of this policy is to provide guidelines for Remote Access IPSec PPTP or L2TP Virtual Private Network (VPN) connections to the Firebrand corporate network.

This policy applies to:

- All Firebrand employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilising VPNs to access the Firebrand network; and
- Implementations of VPN that are directed through an IPSec, PPTP or L2TP Concentrator.

4.1 Policy

Approved Firebrand employees and authorized third parties (customers, vendors, etc.) may utilise the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees unless previously agreed with the Head of IT.

Additionally:

- It is the responsibility of everyone with VPN privileges to ensure that unauthorized users are not allowed access to Firebrand internal networks.
- VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel and all other traffic will be dropped.
- Dual (split) tunnelling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by Firebrand network operational groups.
- All computers connected to Firebrand's internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
- VPN users will be automatically disconnected from Firebrand's network after thirty minutes of inactivity.
    - The user must then logon again to reconnect to the network.

    - Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computers that are not owned by Firebrand must configure the equipment to comply with Firebrand's VPN and Network policies.
- Only MIS-approved VPN clients may be used.
- By using VPN technology with personal equipment, all VPN users are required to understand that machines are an area de facto extension of Firebrand's network, and as such are subject to the same rules and regulations that apply to equipment owned by Firebrand, i.e. each machine must be configured to comply with InfoSec's Security Policies.

4.2 Enforcement

VPN security is an individual responsibility and a failure to abide by this policy may result in disciplinary action.

Authorisation & Document Control

Document Title	Group IT Policy			**Status**	Live
Classification	Internal and external on request	**Last Review**	June 2017	**Next Review**	June 2018
Location	Octopus Portal				

Authorisation	**Responsible Person or Body**
Document Owner	Gordon MacLeod (assisted by Bevan Miller, Head of IT)
Authorised By	Gordon MacLeod

Version History

Version	Author	Issued	Summary of Changes
1.0	Gordon MacLeod	June 2012	First policy
2.0	Gordon MacLeod	June 2017	Review and update of cyber-security guidance and information security elements
3.0	Bevan Miller	June 2017	Amendment of Retention Policy
3.1	Bevan Miller	August 2018	Data Protection clause 1.4.6 update to reference to GDPR