IT and Information Security Policy

Introduction

This policy relates to the use and monitoring of all HTFT Partnership Limited IT infrastructure and communication systems (IT assets). It is intended to promote a legal, safe and secure working environment for all HTFT employees and associates.

HTFT Partnership Limited plc is referred to as 'the Company' in this policy.

Corporate Governance

It is the responsibility of HTFT Partnership Limited to ensure that HTFT, its employees and associates are compliant and that evidence of compliance can be produced should this be requested as part of any internal / external audit.

Corporate Responsibilities

HTFT employees and associates have a responsibility to protect the information entrusted to them by customers and the Company and to ensure that it is used only for its intended purpose and not disclosed to any third party without express permission.

Where Company equipment is provided, it is the responsibility of the recipient to look after such equipment and return it in good working order upon request.

Legal Responsibilities

Computing resources may only be used for lawful purposes. Examples of unlawful use include, but are not limited to, the following:

- Attempting to alter or damage computer equipment, software configurations, or files belonging to the Company, other users, or external networks
- Attempting unauthorised entry to the Company network or external networks
- Intentional or negligent propagation of computer viruses
- Violation of copyright or communications laws
- Violation of software licence agreements
- Transmission of communication which would be considered defamatory
- Transmission of information which would be considered confidential relating to the Company's business or that of its customers to any third-party
- Accessing or attempting to access material which is illegal or inappropriate, including pornographic images

Some of these activities may also constitute criminal offences rendering the individual and/or the Company subject to prosecution.

Ethical Responsibilities

Computing resources must be used in accordance with the ethical standards of the Company. Examples of unethical use (some of which may also have legal consequences) include, but are not limited to, the following:

- Violation of computer system security
- Unauthorised use of computer accounts, access codes, or network identification numbers assigned to others
- Use of computer communications facilities in ways that tie-up, interfere with, or impede computer use of others
- Violation of external networks regulations and policies
- Violation of another user's privacy

Users of IT infrastructure and communication systems

Employees (Permanent & Fixed Term)

The Company will supply standard equipment from the IT catalogue as requested by the line manager at the start of employment or transfer to a different department should there be different requirements. Employees recognised by HR as 'home workers' are responsible for their own broadband procurement and IT support for home broadband connections will not be provided through HTFT.

Associates, Contractors and Third Party Suppliers

All Associates, Contractors and Third Parties who are contracted to work for HTFT must sign a non–disclosure / confidentiality agreement which is retained on file providing they require access to HTFT infrastructure and systems. Contractors or other third parties working for HTFT will adhere to the same security constraints as 'soft associates' and will be treated as such.

For the purposes of this policy we have defined associates as either a 'hard 'Associate or a 'soft' associate.

A 'hard' associate for IT purposes is one who requires access to the following resources:

- Internet
- Full e-mail (including Outlook Wed Access)
- Livedrive

A 'soft' associate for IT purposes is one who only requires limited and short term access to the following resources:

- Internet (provided by the associate themselves)
- E-mail (Only Outlook Web Access is allowed so e-mail has less functionality)

Furthermore "soft" associates will not be provided with HTFT IT supplied equipment by the company.

The Company recommends that 'soft' associates adhere to the following security measures;

- An up to date version of anti-virus software (Sophos, Symantec, Norton etc.) is present and functioning.
- The laptop should be patched to the latest service pack level of the operating system supplied.
- That the associate provides a regular backup of the data on the laptop used.

Temporary/Agency Workers

Temporary/agency workers will be provided with restricted access sufficient to perform their duties. All temporary login accounts will have an expiry date which will need to be reset via the IT Help Desk should their period of employment be extended.

Leavers

All employees, temporary workers and hard associate are obliged to return all IT equipment and software previously issued by the Company. Equipment must not be re-allocated or passed on to anyone else without the knowledge of the IT department.

Corporate Network & Internet Access

The corporate network is the conduit for the passing of all information and data within HTFT. As such it is important that a high level of security is maintained to ensure the network continues to operate effectively as a loss of the whole or parts of the network would have a detrimental impact to business operations.

To this end the following requirements must be adhered to:

- The machine must have an identifiable owner assigned to it. That owner should be present in HTFT's Active Directory.
- The machine must have the latest level of operating system updates, have an up to date anti-virus profile and be encrypted to FIPS 140-2 Level 1 standard or equivalent.

3G /GPRS Dongles (Mobile Broadband)

3G data cards / dongles are issued to employees who need to provide themselves with wireless connectivity in circumstances where normal networks may be inaccessible or unavailable.

In every circumstance where a legitimate network can be securely accessed then this should be the preferred route to take.

If there are alternatives such as home broadband or accessible client networks these should be used instead.

Please do not offer the use of your 3G card to anyone else. It is for company use and should be kept safe and secure at all times while you are travelling.

The actual limit per month set for all 3G Data Cards is 3GB a month per user. Given past statistics it is highly unlikely that this limit will be breached. Nonetheless IT will monitor usage on all cards and will report on any users likely to exceed said limit.

Should IT identify users who demonstrate minimal and infrequent use (across a period of time) they will contact the relevant business with a view to receiving authorisation from the business to cancel said users 3G card or to have it re-assigned to a user that has a greater need.

Electronic Communication Systems

Use of electronic communication systems is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the Company. It should be used in a manner that is consistent with the Company's standards of business and as part of the normal execution of an employee's job responsibilities.

- HTFT Partnership Limited email accounts are provided for all employees, temporary employees and hard associates as required. All business communications must be carried out using the Company's email system and not through personal email accounts. Only in very exceptional circumstances will email accounts in the HTFT email system be configured to forward email to personal email accounts. Should an exception be made then this will require joint authorisation by a director.
- Under no circumstances may the Company's electronic communications systems be used for sending, accessing, receiving or storing any material (text or pictures) in breach of copyright, or of a potentially offensive, discriminatory, harassing, threatening, obscene, political, illegal or defamatory nature. For the purposes of business (other than the Company's business), for chain letters, for spreading gossip or information which is untrue or malicious, or for any purpose that is illegal or against the Company's policies or contrary to the Company's interests.
- Electronic communication systems are to be used for Company business. Limited personal use is considered acceptable providing it complies with this policy and that it does not interfere with an employee's ability to perform his/her assigned duties. Usually this should be restricted to personal break times or before/after working hours. At no time may personal use take priority over business use.
- The Company will directly access employees' email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation or in the case where the employee is absent and the information required is needed for continuance of normal business operations.
- Use of email may be subject to monitoring for security and/or network management reasons.
- Email is not a secure transmission medium. Contents of emails may be intercepted and read by third parties. For this reason, confidential or particularly sensitive information must not be sent by email unless in an appropriately password protected document.
- If contents of e-mails are sensitive then they should be encrypted using the 'Secure Send' facility. This also provides a formal audit trail of files sent and received.
- The distribution of any information through the Company's network is subject to the scrutiny of the Company. The Company reserves the right to determine the suitability of this information.
- All email messages are treated as potential corporate messages of the organisation and will be archived for future retrieval.
- The Company reserves the right to redirect the email of employees that have left for legitimate business purposes. Users are responsible for ensuring personal emails are stopped.

The following is a list of examples of behaviour which are normally regarded as unacceptable. This list is not exhaustive. Users may not:

- Use the corporate systems for online gambling (including National Lottery or similar online gaming), accessing pornography of any description, downloading or distribution of copyright material or software, unauthorised passing on of Company confidential information of any description to external or inappropriate internal sources, passing on of client information to inappropriate sources, non-work related MSN and 'chatting', non-work related 'blogging' or playing computer games in work-time.
- Solicit emails that are unrelated to business activities.

- Send or receive any material that is obscene or defamatory or which is intended to or could have the impact of annoying, harassing or intimidating another person or that are sensitive, emotional or contain potentially offensive content.
- Represent personal opinions as those of the Company.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Company, or the Company itself, without the express permission of the relevant party or otherwise than as authorised to do so in the course of your work.
- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes, customer information and business relationships.
- Send unsolicited bulk email (SPAM) from HTFT's email servers except as authorised to do so in the course of your work.
- Send email through any external email system using a HTFTgroup.co.uk reply-to address (address spoofing).
- Waste time on non-Company business.
- Reply to spam.
- Leave terminal unlocked or logged in when leaving your desk; a malicious user could send messages in your name.
- Avoid 'Mail Storms' - long discussions sent to a distribution list - consider verbal communication or use of a bulletin board.
- The forwarding on of e-mails to Hotmail accounts or private home accounts should only be allowed under exceptional circumstances and with the requisite authorisation of an appropriate board director the audit trail for mail is impaired and general governance of the e-mail system cannot be guaranteed.

Email Archiving

Auto Archive on the computers will enable data collected by automated monitoring tools will not be disclosed to any third-parties except as required by law or as part of any disciplinary investigation. Users of the Company's email services understand and accept that their use of email is being monitored and that data relating to email will be retained within a central database, access to which will be strictly controlled. Details of specific email activity will only be divulged to third parties as part of an ongoing and appropriately authorised investigation, at the request of HR.

You should be aware that merely deleting information may not remove it from the system and deleted material may still be reviewed by the Company and/or disclosed to appropriately authorised third parties.

Social Media, messaging and other Communication Tools

HTFT endorses the value of services such as Facebook, LinkedIn, Twitter, Skype, GoTo meeting, Webex, Ning, instant messaging as social, professional and business tools.

Each of these services has different and evolving security characteristics, so it is important to use them with this knowledge. As a general rule you should assume that these services keep a permanent record of communications and that this is outside the control of HTFT. They should not be used to transmit commercial or sensitive material or as an alternative to the supplied HTFT Partnership Limited e-mail system.

The channels deemed safe for commercial purposes are: telephones, HTFT email, Skype (voice and video but not chat), Webex where HTFT is the organiser.

Corporate IT Systems & Other Software

Access Control: The access to existing systems is altered only when a new starter joins, an employee changes role or an employee leaves the company.

A request form is issued which specifies what access to systems and resources are required by the new starter or the person changing role. The Director will action authorisation to the relevant system. Once done the relevant permissions and access to the systems are set.

For a leaver all credentials are removed within 8 hours of the departure of the leaver.

Microsoft Operating System Support, Update and Patches

HTFT IT will offer support on all Microsoft operating systems that are officially supported by Microsoft via a contract with Microsoft office. (referred to in this document as IT help desk)

Lawful use of software

HTFT Partnership Limited partners with the Federation Against Software Theft (FAST) and takes its legal responsibilities to ensure that all software is appropriately licensed very seriously.

You may not download any software from the Internet onto your Company computer unless authorised to do so. All software must be purchased by the IT department on your behalf and the original media must be catalogued and retained by them. The IT department reserves the right to uninstall any software which contravenes any element of this policy, or which has not been appropriately obtained and licensed. In the event that you cannot contact IT and software deemed necessary for business use needs to be downloaded then it is the responsibility of the requestor to ensure the relevant license is purchased to ensure legal use.

Any software / application downloaded to company equipment that is for personal use only is the responsibility of the individual loading it and said individual assumes any associated liability.

All HTFT computers are subject to periodic software audits to ensure compliance with this policy.

If you believe you require software to perform your duties which is not on your computer, please contact the IT Help Desk in the first instance who will be able to tell you whether this software is authorised and can, with your line manager's approval, make it available to you.

Corporate Equipment

A standard catalogue of IT equipment is maintained. All requests for IT equipment will be fulfilled from the catalogue unless a director approves an alternative purchase. Where an alternative purchase occurs it should be understood that Corporate IT may not support the item moving forwards.

It is the responsibility of each employee using Company assets (IT equipment, mobile phones, etc.), to ensure those assets' proper use and security, whether at home, at a client's premises, or in transit. Such assets are provided for the sole use of HTFT employees and may not be used by family members or other third parties. As with mobile phones, laptops may not be taken on holiday unless there is a business need and only with prior agreement from

your relevant Company Director. Should this authorisation be given then the laptop / mobile if lost or stolen will be replaced at company cost.

Physical Security of Portable Computer Equipment

All items of portable computer equipment (including laptops, PDAs etc.) must be placed in a locked safe, drawer, filing cabinet or similar locked facility outside of normal working hours, with the keys removed and held by the employee or other authorised person.

If portable computer equipment is not left at one of HTFT's offices in this way, then at all times when it is not in the office the equipment must be kept physically secure. It is the individual's responsibility to look after their portable computer equipment and to protect it from loss, theft or damage. Specifically, no equipment must be left unattended in any public space. If it is left in a room such as a meeting room then, if unattended, that room must be locked.

When travelling by car you must keep equipment out of sight in a locked boot. On no account must any equipment be left overnight in a car. If left at an individual's home or other location (e.g. hotel room) then, of course, the same level of care should be taken of the portable equipment as of all other possessions of that employee. If possible, a laptop or other portable equipment should be locked away as if it had been left in the office.

Employees have express permission to take the hardware and software assigned to them off-site and to operate said equipment wherever it is required to fulfil their business responsibilities.

Loss or damage to IT equipment

In the event that any item of IT equipment is lost, stolen or damaged, you must inform the AAT Director at the earliest opportunity. Theft of any item must also be reported to the Police and you should obtain a Crime Reference Number which you must pass on to the Helpdesk.

Business Continuity

This is a low risk due to the fact the computers are not networked, and the data on the computers are saved on to a remote secure serve, with manual back-ups done on a regular basis.

Information Security

Our information and the IT systems that support our business are important assets. The availability, integrity and confidentiality of information are essential if we are to maintain our competitive edge and respected Company reputation.

All information and data relating to HTFT business or the business of any HTFT customer is the property of the Company. Unauthorised duplication, transmission or disclosure is prohibited.

HTFT employees, temporary employees and soft associates must observe the following security measures:

- Ensure that you have Antivirus Software and that it is kept up to date. HTFT-supplied AV software is configured to update whenever the PC is connected to the office network or the Internet. You must, therefore, ensure that you connect your PC or laptop to the office network or the Internet at least fortnightly so that updated virus definition tables can be applied to your local machine.
- Similarly to enable the downloading of windows security patches and updates it would be advisable to ensure that you connect your local device to the office network at least fortnightly.
- Do not open e-mails from an unknown source.
- Do not open attachments you are not expecting.
- Ensure you understand the nature of any sensitive data you may have to work with and that you protect such data at all times from loss or unauthorised disclosure (see below).
- Use effective passwords (see below).
- Do not disclose your password to anyone other than a HTFT IT support analyst, and then only if this is necessary for the resolution of a problem. If you have disclosed your password, change it at the next convenient opportunity.
- Either set a password-protected screen saver or ensure that you lock your PC using the <Windows><L> key combination whenever you leave your computer, even briefly. The protected screen saver should be made operational within 15 minutes of inactivity.
- Ensure that your screen saver is set to activate after 15 minutes of user inactivity.
- Power off your equipment at the end of the working day or before travelling with a laptop.

System Security

No one other than the user has any access to user passwords, quite deliberately so. Consequently, in order to help resolve an IT incident logged by a user, IT may request the user password directly. This will normally be requested verbally.

- Passwords should not be sent by e-mail or given in any written format.
- Once IT has dealt successfully with the incident you should change your password as soon as is practical.
- Where a password is of sufficient length and complexity IT may have to make a note of it. Therefore after the call is resolved IT will destroy any written evidence of the password.
- Where a user password has expired and the IT Helpdesk is contacted for a password reset, IT will seek to validate the user's identity before a password reset can be actioned.
- The IT Help Desk and support employees will always treat user passwords in a strict and confidential manner in compliance with this IT Information Security policy.

Passwords must:

- Be memorable
- Have a minimum of 10 characters
- Contain a mixture of upper and lower case and digits
- Not be disclosed or written down by the password owner (subject to disciplinary action in the case of employed employees or contract termination in the case of contracted associates)
- Not be included in scripts
- Not be easily guessed – no children's, pet's or partner's names, or birthdays etc.
- Be changed regularly and at least every 3 months

These standards will be enforced for all users of HTFT Partnership Limited IT services.

Virus and Malware

Current protection against virus / malware infection is provided by Sophos in the following areas;

- Laptop / Desktop
- All servers
- E-mail systems.

Should an employee suspect that they have become infected (Virus or malware) then this is the security procedure that should be followed;

- Immediately disconnect your laptop
- Contact the IT Help Desk immediately and open a support call.
- Should you be connected remotely to a client at the time, notify them and advise of the actions being carried out locally to assure them this is being dealt with.
- Inform your line manager.
- IT employees will access your machine and clean up the virus / malware.
- Once done IT will raise a security incident via the central ISWG forum.

Should an employee suspect a virus is present on a client environment whilst carrying out remote activity, the following procedure shall be followed;

- Immediately end the remote session then disconnect your laptop / desktop from the corporate network.
- Contact the IT Help Desk straight away and open a support call.
- Contact the client to notify them of the virus warning and advise that remote access to their systems will cease until written confirmation is received from their IT department ensuring the threat has been dealt with.
- Inform your line manager who will advise staff internally not to connect to the client until further notice.
- IT employees will access your machine and clean up the virus / malware.

On receipt of written confirmation of the removal, the recipients should pass the information on to the helpdesk so they can update the incident for subsequent review and closure. Once approved, both customer and colleagues will be notified allowing remote activity to commence once again.

Corporate Backup Policy

Corporate backup policy consists of two distinct phases;

- Data that is backed up on-site at locations
- Copies of backup data held off-site (normally used for Business Continuity purposes)

A backup copy of data is in itself a temporary arrangement and therefore has a ‘finite’ life.

If the business wishes to keep data for a long period of time then an archive system should be used.

Personal data backup

Corporate IT provides a backup service for all laptop and office based desktops using a product called Livedrive remote server. This product is installed for all users and operates in the background without unduly affecting the user. It backs up against a general profile and sends a copy of data on the selected device to a centrally held encrypted data store. The general profile caters for backing up most types of file but there are certain exemptions.

Clear Working Environment

We are required to protect and secure items that may be deemed 'sensitive'. It works to support the CESG guidelines. The following areas/items are covered:

- Desks
- Workstations
- Computer screens / monitors
- Whiteboards
- Meeting Rooms
- Public areas.
- Printers
- Photocopiers
- Scanners
- Flipcharts

Normal working hours are defined as 0800-2100 from Monday to Sunday inclusive. Outside of these hours all sensitive information (whether marked or not) will be stored in lockable storage units.

- During working hours sensitive information shall be concealed if desks are left unattended.
- Classified information will not be placed in bins under desks or in offices at any time. Classified information will be placed in an approved confidential waste container.
- Documents will be immediately retrieved from printers/copiers/scanners and fax machines.
- Outside normal office hours, all desktop and laptop computers must be closed down unless required to remain on for operational purposes. If this is the case, screens should be locked, with passwords enabled, when the employee is not at his/her desk.
- Laptop computers, mobile telephones and other portable assets will be locked away outside of normal office hours unless required for operational purposes.
- Those in charge of meetings will ensure no sensitive information is left in meetings rooms/venues. This includes media left on the table, slides, flip-charts or whiteboards.
- Locked offices and restricted areas do not exempt the occupiers from complying with this Clear Working Environment Policy.
- Management will ensure that employees have suitable lockable storage facilities to enable them to comply with this Clear Working Environment Policy.
- Management will ensure that full co-operation is given to the Security Forum to enable audits to be undertaken.

The requirements outlined above represent the minimum standards expected of all HTFT employees working with sensitive data. Access to some classes of data (for example information relating to offenders or vulnerable young

people) may require additional measures (for example CRB checks) which will be communicated and monitored by individual business units. Employees and associates must also observe any security policies or procedures required by HTFT clients.

Security Incident

A security incident is an event that threatens the confidentiality of data or documents, their integrity in terms of them being reliable and trustworthy or their availability in terms of them being accessible to the right people at the right time of need.

Examples of such are;

- An electronic attack (whether successful or not)
- Loss of data (whether intentional or not)
- Loss of any control method as defined in this security policy (i.e. any of the don'ts listed)
- Attempts to access systems, services data or company resources illegitimately.
- Anything that is deemed to be an incident by a member of a HTFT security forum.
- Discovery of sensitive material or an electronic device (such as USB memory stick or backup drive) left unattended whether intentional or not.

If in doubt please report the incident to your Director.

Once classified as a security incident it will be logged on the appropriate system the Director will perform the following;

- Logging the incident and assigning an incident number
- Investigating the incident involving any necessary parties
- Making other security members aware of the incident.
- Keeping a note of all documentation and any pertinent evidence.
- Making recommendations to improve the situation.
- Notifying any of the appropriate authorities (Police, Fire etc) if relevant.
- In the event of discovery of unattended items that are safe to handle (i.e. electronic items laptops, memory sticks etc.) then these should be handed to the IT department.
- If unsure about an item (i.e. a suspicious looking parcel oddly situated contact the Facilities department who will take the appropriate course of action).
- Relevant updates and closure of the incident.

Consequences of Non Compliance with this Policy

- All instances and acts which are in breach of this policy will be taken seriously, will be investigated thoroughly and fairly in line with the Company's disciplinary procedure and may lead to disciplinary action up to and including dismissal.