Information Technology Policy

CONTENTS

Information Technology Policy Statement

Computer Policy

Software

System Integrity

Data Integrity

Security

Additional considerations for Portable Computers\Smartphones\Tablets

E-mail Policy

Internet Policy

Telephone Policy

Aberdeen Office (Head Office)
Twin Spires Business Units
Mugiemoss Road
Aberdeen
AB21 9NY
T: 01224 698288 E: email@gtfsl.co.uk

Livingston Office
The Hub, Rankine Square
Deans South West Industrial Estate
Livingston
EH54 8SH
T: 01506 469142 E: livingston@gtfsl.co.uk

www.gtfsl.co.uk

Company No: SC151272
VAT No: GB 605 2597 45

Information Technology Policy Statement

The Company is committed to the use of Information Technology (IT) for business purposes. It must ensure however that suitable measures are in place to prevent security breaches and other negative consequences.

The purpose of the policies below is to ensure that all employees are aware of how they are required to use the Company's IT facilities and the data stored upon them:

- Computer Policy
- E-mail Policy
- Internet Policy
- Telephone Policy

The policies promote an effective, efficient, and ethical environment that reduces the risk of the Company and individual employees to disruption in service and legal liability.

The Company's IT facilities comprise, without limitation, any hardware, software, telecommunications and supporting infrastructure used to manage and deliver data and voice.

Within the scope of these policies, data is defined as the information managed by the Computer as opposed to the program (software) that decides what action the Computer should take. Data includes, but is not limited to, all Company, employee, customer and third-party information held in electronic form.

Electronic forms of data storage include all data files, email, graphic files, sound and video files, whether or not compiled or compressed.

The Company reserves the right to audit, monitor or record, using any method it deems reasonable, any part of the IT facilities including all electronically stored data. Reasons for doing this include, but are not limited to, the following:

- Establish compliance with Company Policies;
- Establish the existence of facts;
- Determine or demonstrate standards which are or ought to be achieved (quality control and training);
- Prevent, investigate or detect crime and disciplinary offences;
- Investigate or detect unauthorised or illicit use of the IT facilities;
- Maintain effective system operation;
- Determine whether communications are relevant to the business or are personal communications.

A non-exhaustive list of examples of monitoring that may be carried out by the Company includes:

1. Recording images by means of CCTV cameras, either so that the recordings can be viewed routinely to ensure that health and safety rules are being complied with, or to check the physical security of the Company's premises and ensure the security of employees;

2. Opening employees' data files (such as e-mails or listening to their voice-mails) to look for evidence of malpractice;

3.Using automated checking software to collect information about employees (e.g. to find out whether employees are sending or receiving inappropriate e-mails);

4.Examining logs of websites visited to check that individual employees are not downloading material from unauthorised websites;

5.Keeping records of telephone calls made to or from Company telephones, either to listen to as part of employee's training, or to simply have a record to refer to in the event of a customer complaint about an employee;

6.Systematically checking logs of telephone numbers called to detect premium-rate lines.

All auditing, monitoring and recording activities will be conducted by authorised personnel only and in strict compliance with internal Company procedures. In determining the appropriateness of any auditing, monitoring or recording activities conducted by the Company a documented Impact Assessment will be made that includes identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver:

1.Identifying any likely adverse impact of the monitoring arrangement such as intrusion into workers 'private lives or private correspondence;

2.Considering alternatives to monitoring or different ways in which it might be carried out. Alternatives might include improved training, communication or supervision. Monitoring could be limited to specific employees, where there are allegations or suspicions of wrongdoing. Spot checks could replace continuous monitoring;

3.Taking into account the obligations that arise from monitoring. These include requirements to: inform employees; keep information securely; limit those who have authority to carry out monitoring and have them subject to confidentiality and security rules;

4.Judging whether monitoring is justified, weighing the benefits against any adverse impact. Intrusion will only be justified if there is a risk of serious damage to the business.

By using Company IT facilities you consent to all Company auditing, monitoring and recording activities and agree to cooperate fully in any related activities. The Company reserves the right to temporarily or permanently limit, withdraw or restrict use of, or access to, any IT facilities and/or data if they are used, in the Company's sole opinion, in an inappropriate matter. Breach of these policies and/or misuse of the Company's IT facilities is a disciplinary offence and, in appropriate circumstances, will lead to disciplinary action being taken against the individual, up to and including summary dismissal.

Computer Policy

As well as desktop PCs, laptops and servers, the Company computers comprise, without limitation, Personal Digital Assistants (PDA), Mobile Telephones and any other device that is capable of storing software and/or data.

Software

The following points must be adhered to at all times:

1.All software must be approved for use by the Head of IT or Deputy in advance of it being installed on any of the Company's computers.

2.It is not permitted to use software on Company computers for which the Company does not have the necessary licence.

All authorised software must be used in accordance with the licensing conditions.
3.Software received from a source other than the IT Department must be given to a member of the It Department prior to installation so that compatibility and licensing conditions may be verified and software records updated. The IT Department may choose to retain the software and/or licences.

4.Where it is possible to do so, software must not be installed on any of the Company's computers without first having been scanned for viruses. In the event of a virus being detected, a member of the It Department must be contacted before proceeding with the installation.

5.You must not make any copies of software, including configuration files, either from installation/backup media or from a Computer itself without the prior approval of a member of the It Department. The IT Department retains all legally-permitted back-up copies of all software used in the business and it should not be necessary for you to make copies for back-up purposes.

6.The Company is committed to the Federation Against Software Theft (FAST) Standard for Software Compliance. If software is found to be used illegally on Company IT facilities, not only could the Company face a criminal investigation but individual employees may be subject to criminal prosecution.

7.If you learn of any misuse of software within the organisation you must notify a member of the IT Department or a registered Director of the Company.

8.To enforce this policy the Company will perform regular software audits.

System Integrity

To ensure the integrity of our system the following points are to be adhered:

1.It is the responsibility of every employee to take all reasonable precautions to safeguard the Company's IT facilities from physical hazards, e.g. liquid spillages and blocked ventilation grills.

2.An anti-virus software package is installed on every laptop and desktop PC and you should run this package to check removable media (such as floppy disks or USB pen drives) is virus free before you use it. If in doubt as to its use, contact the IT Department.

3.In the event of a virus being detected on any removable media you must eject the media from the computer, disconnect the computer from the network (where applicable) and contact the IT Department for further guidance.

4. In the event of a virus being detected on a computer you must disconnect the computer from the network (if connected) and contact a member of the IT Department for further guidance.

5. It is becoming increasingly common for music/movie CDs and DVDs to contain self-installing, sometimes hidden, computer programs. Non-business related CDs and DVDs must not be used with Company computers without the prior approval of a member of the IT Department. All business related and other permitted music/movie CDs and DVDs must be virus scanned and found virus free before use. In the event that you think a program might have inadvertently been installed on your computer please contact a member of the IT Department.

6. It is not permitted to connect any hardware which the Company does not own to any of the Company owned IT facilities without the prior approval of a member of the IT Department. This includes, but is not limited to, portable music players, wireless keyboards/mice and other computers.

7. Only personnel authorised to do so by a member of the IT Department may connect equipment authorised by the IT Department to Company IT facilities.

8. You may only alter the configuration settings of a Company computer in line with Company guidelines referred to in PC/Laptop Awareness guidelines, stored on the shared network drive. These settings include the screensaver, background image, mouse pointer and sounds. All other configuration settings must not be changed without obtaining prior authorisation from a member of the IT Department. If in any doubt about what settings can be changed on a Computer please seek guidance from the IT Department.

9. No office-based IT facilities may be removed from Company premises without the prior authorisation of a member of the IT Department.

10. No IT facilities may be re-allocated without the prior approval of a member of the IT Department.

11. Only personnel authorised by the Head of IT or Deputy may dispose of Company IT facilities.

Data Integrity

An ‘information asset’ is defined as information which has, or will have, value to the Company. Data encompasses all information assets and all personal information stored electronically on any of the Company’s IT facilities. Data has varying degrees of sensitivity and importance. Security classifications and associated protective measures are necessary to protect the business and individuals from unauthorised access.

All data held on Company IT facilities must be assigned to one of the following 4 security classifications:

• Confidential – information assets to which only a limited number of employees should have access.
• Internal – information assets, which may be accessible to all employees of the Company – but not to people outside the Company and not to third parties working in-house.
• Personal – information stored on Company IT facilities by an individual for purposes other than the Company's business. An example of this may be a letter to a bank manager.
• Public – all information assets not included in the above three categories.

To ensure data integrity the following points must also be adhered to:

1. Confidential and Internal data covers all information not in the public domain, or information in the public domain that the Company considers propriety information, the disclosure, alteration or misuse of which may cause damage to the Company, such as loss of profit or competitive advantage.

2. Public data does not mean that everyone should be provided with access to the information, rather that it would not mean damage in any of the above mentioned ways if it was accessed.

3. The Company endeavours to maintain an inventory of all electronically stored information assets, excluding data. In the event of creating or using an information asset that is not recorded in the inventory you must inform your line manager of the asset and together determine its security classification so that the inventory may be updated.

4. The Company reserves the right to monitor and to access all data accessed, created, modified, duplicated, stored or distributed by its IT facilities. You must not attempt to view, create, modify or delete data for which you have no authorisation to do so.

5. You must not store Confidential data in areas on the Company network that enable it to be retrieved by anyone other than authorised personnel, unless it has been encrypted or password protected.

6. Confidential information must not be stored on the local drives of office based desktop PCs as other persons could access the computer and gain access to the information.

7. Consideration should be given to further protecting Confidential data by means of data encryption and/or password protection.

8. You must not use or make copies of, including in hardcopy format, any data for your own unauthorised use. Additionally, you must not provide copies of any data, including in hardcopy format, to anyone else unless authorised to do so as part of your job.

9. It is Company policy not to use external hard drives, zip drives and internal SD disks to store data, but you should only use the company network drives, or cloud facilities provided by the Company for data storage. Please do not store any data on a local computer, and certainly not on a non-Company computer system.

10. In exceptional circumstances, you may be required to save data to an external source (9 above). Removable media must be password protected or encrypted.

11. Be aware that it may still be possible to access data that has been deleted. It is essential therefore that when authorised by a member of the IT Department to dispose of storage media that you physically destroy it to ensure that it cannot be used again.

12. Password protected screen savers must be used to secure your computer when leaving it unattended, and should be set to operate automatically after ten minutes of inactivity.

13. Company IT facilities must not be used to access, create, duplicate, store or distribute in any form, by any means, data that is, or may be considered:

14. Illegal, pornographic, abusive, sexist, racist, bigoted, defamatory, offensive, harassing, intimidating, or advocating a religious or political cause

15. Please refer to the Equal Opportunities Policy statement in the Staff Handbook for clarification.

16. Use of the Company's IT facilities to maintain Personal data is subject to the Company's right to monitor the system for its legitimate business purposes, and by choosing to use the Company's facilities for the maintenance of Personal data you consent to the company monitoring such data.

17. Where possible, Personal information should be stored within a folder named 'Private'

18. Certain data has to be retained for specific periods of time for legislative and/or Company reasons. This is defined within the Company "Information Retention Schedule"

19. All hardcopy printouts of electronically stored information assets are subject to the Company policy for Information Labelling and Handling.

20. When introducing data from an external source, ensure that virus scanning is performed and that all copyright restrictions are obeyed i.e. the Company is permitted by law to access, store, modify or distribute as appropriate the data you are introducing to Company IT facilities.

Security

To ensure the security of our IT systems, it is important to follow the following measures:

1. Under no circumstances should you attempt to access Company systems from an untrusted network (non-Company) without first ensuring you have the Company Virtual Private Network (VPN) connectivity enabled. If you are in any doubt about this, please contact IT Service Desk.

2. Security measures are an important element in preserving the integrity of systems and data. It is therefore essential that the following are observed at all times:

3. Where you are issued with a personal login account (either a PIN or a unique ID and password) you are responsible for the actions performed under that login account.

4. You must not allow your personal login account to be used by another person without authorisation.

5. You must not use anyone else's personal login account without authorisation.

6. You must keep your personal login account passwords confidential and change them regularly in accordance with Group rules.

7. The only person you may disclose your personal login account password to is a member of the IT Department or a member of staff authorised by the Human Resources department. After disclosure and completion of all necessary work on your PC or laptop, you must change your password.

8. Where you are issued with a shared login account (shared PIN or shared ID and password) you may only disclose the PIN or password to other members of the group authorised to have access, otherwise the same disclosure rules as for a personal login account apply.

9. If you have reason to believe the secrecy of your personal login account has been compromised, you should immediately change your PIN or Password and contact the IT Department.

10. If you have reason to believe a shared login account has been compromised, you should immediately contact the IT Department.

11. You must not attempt to use any computer or any software application for any other purpose than has been authorised.

12. Use, on or in connection with any part of the Company's IT facilities, of programs, utilities and/or other devices designed to:

- Bypass security measures.
- Determine or identify passwords, or
- Breach conditional access systems, without the prior authorisation of the Head of IT or a registered Company Director is not permitted.

13. Use of remote access applications such as VNC and PC Anywhere to obtain unauthorised access to another computer is not permitted.

14. If you have a legitimate business need to access systems or data for which you do not have authorisation, you must formally apply for access. For guidance on how to do this please contact a member of the IT Department.

15. When leaving your computer unattended you must ensure that you either log out or lock the computer screen to prevent unauthorised use in your absence.

16. Only personnel authorised to do so by a member of the IT Department may enter areas designated as an 'IT Restricted Area'.

Additional considerations for Portable Computers\Smartphones\Tablets

Other considerations should be:

1. When accessing the Company's IT facilities remotely, do not use login scripts that contain passwords or other information of use to hackers.

2. Use a carry case to reduce the risk of accidental damage.

3. Always store portable computers securely when not in use.

4. Where possible, use a Kensington lock or similar to secure your computer to your work area.

5. When leaving a computer in a vehicle ensure that it is stored in the boot and is out if sight.

6. Be vigilant in public places, as theft of portable computers is common.

7. Do not view sensitive information in a public place where the screen could be overlooked.

8. Give serious consideration to where you site any device holders / recharging equipment in your car. The visible presence of these significantly increases the risk of a car being broken into.

9. You must ensure that regular backups of your data are made. Use the Company provided replication services whenever possible. All removable media containing sensitive information must be stored securely.

10. Sensitive information should not be held on the internal storage media of any device for any longer than is absolutely necessary.

11. Use the security measures available on the device, such as the setting of PIN numbers and passwords, to protect the data held on them.

12. Never loan a portable computer to anyone, including other employees of the company, without prior approval from IT Department as the recipient will have access to all the information stored upon it and his may compromise data confidentiality.

13. When using a portable device to access the Internet, observe the Company's Internet policy at all times.

14. When using a portable device to send messages, observe the Company's Email policy at all times.

15. Many services available to mobile computer users, including text messaging, WAP sessions, information services and ring tones are charged to the Company when they are used. You must not use any such services without the prior written approval of your line manager. Besides any

disciplinary action that may arise, the Company reserves the right to pass on to you any charges incurred by the Company for unauthorised use.

E-mail Policy

Whenever applicable, references to e-mail should also be taken to cover Text Messages, Picture Messages and any other messaging formats that Company IT facilities are capable of sending and/or receiving. Please note this applies equally to Social Media (Facebook, LinkedIn, etc.). To ensure quality and conformity the following guidelines must be followed:

1. The Company reserves the right to monitor and to access any messages within its IT facilities.

2. The layout of e-mails should follow the guidelines of the Company Design System (VDI).

3. All e-mails must include the Company's disclaimer in full.

4. The same caution should be exercised when sending an e-mail as with written communications.

5. You must never send messages using Company IT facilities that are considered inappropriate, regardless of whether the material is addressed to recipients inside or outside of the Company. Improper statements can give rise to legal action against you and/or the Company. Please refer to the Equal Opportunities Policy statement in the Staff Handbook for further clarification.

6. In general, e-mail may be used a. For internal communications, e.g. instead of letters, memos, notices of meetings and minutes of meetings

b. For external communications when legal or other important physical documentation is not required

c. Instead of leaving a message in a voice mailbox

7. In general, e-mail should not be used a. If a formal document is needed e.g. from a legal point of view

b. If direct dialogue with the person in question is needed or preferable

8. If the person needs to be contacted immediately Remember that advice given by e-mail may be relied upon and contracts may be created by e-mail. Be aware that e-mail messages, however confidential or damaging, may have to be disclosed in court proceedings if relevant to the issues. The mere deletion of a message or file may not fully eliminate it from the system – it may be traced and retrieved at a later date

9. Confidential information sent within the Microsoft Exchange/Outlook environment must be encrypted and signed. The subject field must begin *** CONFIDENTIAL ***: and the Mood Stamp must also be used to indicate the classification of the message. The email should only be sent to recipients that are authorised to see the information.

10. E-mail messages sent externally may be accessed by others. Lotus Notes e-mail is not encrypted – even if you choose to encrypt it by using Lotus Notes internal encryption, it is decrypted once it gets outside of the Company. Confidential and/or Internal data must not be distributed by external e-mail unless it has been encrypted using a method approved by the IT Department.

11. Care should be taken when you receive a message that has been forwarded to you. Authenticity of forwarded messages cannot always be guaranteed.

12. While it is accepted that you may wish to send personal messages from time to time, you should respect the primary purpose of the e-mail system is for business use and keep personal use to a minimum.

13. Use of the e-mail system for personal messages is subject to the company's right to monitor the system for its legitimate business purposes, and by choosing to use the company's e-mail system to send a personal message you consent to the company monitoring such messages (including where it is sent using a computer off-site).

14. Do not create e-mail congestion by replying with attachments intact or retaining message history when it is unnecessary, sending trivial messages, forwarding "chain letters" or unnecessarily copying people into e-mails.

15. Never detach or launch file attachments (even what looks like an innocuous TXT file can be a disguised virus or Trojan) or click on links from unknown correspondents without first having contacted a member of the IT Department for advice.

16. In order to prevent impaired system performance as a result of the space taken by large attached files being received and subsequently circulated, consideration should always be given to locating large files on the network and emailing only a link to the file rather than the file itself.

17. You are expected to maintain your mailbox regularly, deleting unwanted messages and saving attachments to your network drive before deleting the attachment out of your mailbox.

18. There are four different categories of Internet and e-mail use. You should be aware that misuse of e-mail can result in disciplinary action against you, up to and including summary dismissal.

19. Should an employee receive what they feel to be offensive, unpleasant, harassing or otherwise intimidating messages via e-mail, they should immediately inform the Human Resources department or any member of local management. This incident will then be investigated in accordance with the relevant policies detailed in the Staff Handbook

20.Any e-mail accounts provided to you as part of a Company financed home Internet connection are subject to this policy.

Internet Policy

Whenever applicable, references to the Internet should also be taken to cover WAP and all other external information systems that Company IT facilities are capable of accessing.

The Internet facility is provided entirely at the discretion of the Company and is not a contractual benefit. It may be withdrawn at any stage. Any breach of this policy may result in disciplinary action, up to and including summary dismissal.

The company reserves the right to monitor the system for its legitimate business purposes, and by choosing to use the Company's IT facilities, you consent to the Company monitoring all Internet sites you access.

Internet activity (including e-mail) is generally grouped into four categories as follows:

1. Business use: web-sites used in the performance of Company duties.

2. Non-business but acceptable use: responsible personal use in a time acceptable to the employee's line manager, including, but not limited to, web-sites such as news, weather, travel information, Internet shopping and e-mail.

3. Inappropriate use: this includes but is not limited to time spent on category (b) usage that interferes with business duties, large non-business related downloads including the streaming of music/video, on-line gaming, non-business related chatrooms/bulletin boards and the deliberate introduction of unauthorised software onto Company IT facilities.

4. Misuse: this includes but is not limited to accessing, downloading or distributing material defined as inappropriate in section 4.8.1.3, and including soliciting money or sending unsolicited e-mail (the practice known as 'spamming').

Disciplinary action (which could result in dismissal) can be taken against an employee where usage falls into the categories listed in (3) and (4) above.

If in any doubt as to whether an activity you wish to engage in may constitute Misuse or Inappropriate use then please refer to the Equal Opportunities Policy statement in the Staff Handbook and seek guidance from a member of the IT Department and/or the HR department.

Should you erroneously access an inappropriate site or download a program please advise the IT Department.

Where material is obtained from the Internet, you must ensure that any copyright restrictions are obeyed and that virus protection procedures are followed.

When not in use, please ensure you close down all internet applications.

Please bear in mind that security cannot be guaranteed when paying for goods or services using a credit card via the Internet. Consequently, visiting sites for non-business purposes that require disclosure of your

personal credit card details is undertaken entirely at your own risk, and you should take the necessary precautions to protect this information accordingly.

Use of Social Networking sites should be kept to a minimum, and for business use only. All communication within Social Networking sites must be business-like and comply with Company rules.

Telephone Policy

The Company's telephone system includes both office-based and mobile telephones. While it is accepted that you may need to use the Company's telephone system to make personal calls from time to time, you should respect the primary purpose of the telephone system is for business use and keep personal calls to a minimum.

Use of the telephone system for personal calls is subject to the Company's right to monitor the system for its legitimate business purposes, and by choosing to use the Company's telephone system to make a personal call you consent to the Company recording the number and/or monitoring of such a call. Anyone who makes persistent use of the telephone system for personal calls will be asked to provide an explanation.

The Company reserves the right, if appropriate, to claim reimbursement for all personal calls made. For all Mobile Devices, please refer to Space Solutions Mobile Policy.

Signed

John Morrison
Managing Director
4th Nov 2022

DATE	REVISION	DETAIL	PREPARED BY	APROVED BY
Nov 2022			John Dunn	John Morrison