IT Policy

Incorporating Computer Use Policy

Contents

Introduction

This policy is designed to give staff guidance on all aspects of IT usage. It will provide details of all the IT systems and the individual user’s responsibility to use systems safely and in line with organisational policy and procedures.

The policy is extended to include telephony and any other systems administered by the IT Premises team.

Standguide needs to make staff aware of acceptable and unacceptable uses of systems, equipment and other IT related matters.

This policy should be read in conjunction with the Social Media Policy and the Employee Handbook.

This policy also covers customer use of Standguide machines and use of any personal device with Internet access.

1 Network Accounts

Usernames & Passwords

Each user is issued with a username and password. The password must not be disclosed to anybody under any circumstances. Any such disclosure may constitute a disciplinary offence which may lead to dismissal.

Each user is responsible for keeping their individual username and password secure. Staff must not share their username or password with anyone. If a breach of security is recorded under your login, the burden of proof will be with you to show that you are not responsible for the breach and any effects it had.

Intentionally introducing files that cause computer problems could be prosecutable under the Misuse of Computers Act.

File Server

Each user is allocated a personal area (OneDrive) which resides in the main Standguide Office 365 cloud system. Access to this area is allowed only to the named user. Users should usually, however, save contract specific documents and files in the appropriate area on the SharePoint system.

If there is a suspicion of any misconduct, a Standguide Director may allow a line manager access to an individual's personal storage area.

All the data kept on the file server is regularly backed-up. This provides a fairly robust method of recovering lost data, but it is not an absolutely guaranteed process.

2 Computer Hardware

The following apply to all computer hardware:

- All computer hardware is the property of Standguide and is subject to auditing regulations.
- Any computer device (computer; laptop; mobile phone; stand alone or networked PC, etc.) is considered 'Computer Hardware'.
- Each user is responsible for the computer (and any attached peripherals) allocated to him/her.
- This equipment is provided to Standguide personnel for use on Standguide business only.
- Hardware requirements must be agreed by line managers before the IT Infrastructure Manager is approached for ordering and installing new computer systems. Generally, standardised equipment will be issued.

You cannot without the explicit agreement of the IT Infrastructure Manager:

- Install or remove hardware components of any computer system.
- Move hardware components from one computer system to another.
- Reallocate equipment to another user.
- Connect any personal equipment to computer hardware or the Standguide computer network (e.g. digital camera, mobile phone, laptop, etc.).

Line managers must request new equipment on behalf of their staff and must consult with the IT Infrastructure Manager during the planning process. The IT Infrastructure Manager will ultimately be responsible for supporting the ordering, installation and use of the equipment. The IT Infrastructure Manager will try to give an accurate timescale and likely cost on this process at the consultation stage with the line manager.

3 Portable (Notebook / Laptop) Computers

Portable computing equipment is provided to users that have a specific need to remotely access data and email. This includes permanently enabled remote workers and colleagues who have an occasional need to access services remotely, who can book out equipment from the IT Premises team when the need arises.

Bookable Equipment for Meetings (Head Office only)

Head Office reception maintains a single laptop and data projector which staff may book for meetings. All requests should be sent via email to reception@standguide.co.uk or by telephone. Please note this resource is limited and loan periods are meant to be for short periods (maximum of 1 day).

- The laptop will be provided with a universal local login (e.g. user). The password will be provided on collection of the equipment.

- Staff are responsible for removing all presentations from the laptops and correctly packing equipment away before returning the equipment to reception.

4 Printing

There are currently varying levels of printer service within Standguide – Head Office, offices based within Serviced Buildings and offices leased/owned by Standguide.

Staff based in Head Office or in centres are generally provided with access to a networked printer and not local printers associated with specific computer equipment. This facilitates printing and assures that resources are efficiently shared between users. In the event of a problem with a network printer, contact the IT Infrastructure Manager to report a fault.

Staff can send documents to any network printer as long as the correct printer driver software has been added to their computer for use. Contact the IT Infrastructure Manager if you have problems connecting to a printer.

Every colleague has the responsibility for basic printer maintenance consisting of loading the printer with the appropriate paper and changing the necessary toner cartridges. A nominated colleague should order printer cartridges when necessary (via Head Office reception).

Any requests for the purchase of printers must be agreed with the IT Infrastructure Manager.

5 Computer Software

All Standguide computer systems provide the following applications: Operating System (Windows 7, 8 or 10), MS Word, MS Excel, MS Power Point and MS Outlook (latest versions). An antivirus solution is also provided. Staff using laptops should regularly connect their laptop to the internet in order to ensure that critical and high priority software updates are downloaded and installed onto their system.

No other software (free or commercial) should be installed without the agreement of the IT Infrastructure Manager. Purchasing of all software will be via the IT Infrastructure Manager who will arrange for the installation and configuration and will keep the original disc(s) for auditing purposes.

Any software used to download music or to store music may, although it is freeware, contravene copyright laws. Any user found to have this software will have it removed and all files (e.g. songs, etc.) will be deleted.

Any software other than those that are installed as a standard may cause problems with the operation of that computer, and as such the line manager should make any request to install such software to the IT Infrastructure Manager as long as it is wholly required in order for that colleague to perform their duties.

The IT Infrastructure Manager will have the right to audit computers for unauthorised use of software, and these will be carried out periodically, with unauthorised software likely to be removed. Unauthorised software may cause problems with license agreements or contain spyware that may compromise the organisation's computer equipment or network.

6 Internet

As a progressive organisation, Standguide recognises the importance of the internet and email facilities to our business. The internet is a valuable resource for research and email is essential to communication in the present-day corporate environment. There is an obligation to use these systems responsibly, ensuring compliance with the Data Protection Act 2018, The Computer Misuse Act 1990 and The Human Rights Act 1998. We should always remember that the internet is a tool with inherent security risks and without guarantees of reliability or performance.

Inappropriate use

No member of staff is permitted to access, display or download from internet sites that hold offensive material. To do so, is considered a serious breach of Standguide's policy and may result in disciplinary action. Examples of what is considered offensive material include hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, extremist or terrorist materials, religious or political opinions and disability. This list is not exhaustive.

Other than instances which demand criminal prosecution, your employer is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the internet. Ask your line manager for advice if in any doubt.

Copyrighted material must only be used in accordance with the laws which protect copyright, designs and patents.

Use of the internet facility for commercial activities other than in the conduct of the organisation's business is prohibited.

Use of the internet facility for political activities is prohibited.

If you accidentally connect to such a site, disconnect immediately and inform your line manager or the IT Infrastructure Manager. Failure to do so may incriminate you.

If you join a chat group, news group, post messages on a bulletin board or social media, you are expected to conduct yourself in an honest and professional manner. You are responsible for what you write; ***you should be courteous and inoffensive***. Unless you are authorised to do so, you are not permitted to write or present views on behalf of Standguide. This means that you cannot join a chat group in the name of Standguide, nor can you design a web site and publish it under the name of the organisation. This could lead to disciplinary action and potentially dismissal.

(See appendices for examples of acceptable and unacceptable use)

Personal Use

Access to the internet is provided primarily for business need - that is for work or for professional development and training.

Reasonable personal use may be permitted during designated breaks provided this does not interfere with the performance of your duties.

Personal access to the internet can be limited or denied by your manager. Staff must act in accordance with their manager's decision.

Monitoring

Standguide reserves the right, consistent with UK law, to monitor all internet access.

The internet is a major source of computer viruses the effects of which can range from a minor irritant to a major disaster and all have costs involved in their eradication. Although most IT networks have background antivirus defences, it is still essential for users to specifically check files and mail prior to opening. If a user suspects a virus infestation they must stop using that machine and contact the IT Infrastructure Manager immediately.

Information obtained through the internet may not be accurate, and staff must check the accuracy, adequacy or completeness of any such information.

7 Email

Email is an invaluable tool that is essential for communication in the present-day corporate environment; however, it should be recognised that it can be a dangerous medium and should be used with care and caution. The use of the organisation's email facilities by all individuals assumes and implies compliance with this policy. There are no exceptions. It is worthwhile pointing out that use of Standguide provided email accounts are not for personal use. The contents of these accounts are always the property of Standguide.

Remember that all laws relating to written communications also apply to email messages.

With the weakness of traditional emails in mind, Standguide must ensure that no information that could be deemed as confidential or PROTECTED should be sent via email without proper checks and security controls being in place. The key areas for all employees to consider when sending emails are:

a) Is the information being sent of a confidential and PROTECTED status?
b) Does the information being sent constitute a breach of Information Security if it is accessed by an unauthorised person or persons?
c) Is the recipient of the email authorised to view this information?
d) Does the recipient know and adhere to the PROTECTED nature of the information?
e) Is the information being sent secure and free from the dangers of interception?

In short, if the answer to points a and b are "yes", and any of the remaining questions are "no", the email should not be sent.

Where it is established through points c and d above, that the recipient of the email is authorised and adheres to the PROTECTED nature of the information being sent, appropriate encryption must be applied to the information before it is sent. Standguide will use the software package 7-ZIP which uses the AES 256bit encryption. This is suitable for encrypting messages, conforms to FIPS 140-2, and provides sufficient security to avoid a security breach on interception.

A key element of using 7-ZIP though is the setting of passwords and release of these to the recipient of the email sent. The password should be set as per the Standguide Password Rules in Annex A of this policy, should not be the same password as the logon details, and should only be used once. This password must be communicated to the recipient of the email before they can access the information within it. It should not be emailed, as this runs the risk of being intercepted, but should be communicated by telephone, letter or SMS instead.

At no time should any confidential customer information be transmitted in the body of an email message or in an unencrypted format. To do so would place the security of the information at risk. This would be defined as a security breach, and action taken against the sender of the email in question.

Email is provided to employees of Standguide as an essential business tool. It is expected that all employees should treat this as such and should not expose the security of Standguide through the intentional sending and receiving of inappropriate, malicious, or damaging emails and attachments. Our mail server is configured to detect and prevent such emails and messaging, and logs will be inspected to ascertain misuse of this resource

Virus Protection

Email is a major transmitter of computer viruses the effects of which can range from a minor irritation to a major disaster. Any type of virus has costs involved in its eradication. Although the email system has background antivirus defences, it is still essential for users to specifically check any suspicious mail or attachments prior to opening.

Colleagues should not send messages to all users without approval from the IT Infrastructure Manager (especially Communications & Marketing) or a Standguide Director.

On no account should individuals send or forward virus warnings to other users. Warnings should be passed to the IT Infrastructure Manager, who has the means to check if these warnings are hoaxes (which they invariably are). If it is a genuine warning, the IT Infrastructure Manager will take all measures to protect the corporate IT infrastructure and inform colleagues if required. In the event that a user suspects a virus attack, they must stop using that machine and contact the IT Infrastructure Manager or Axon-IT immediately.

Unacceptable Use

Unacceptable use of email is considered a serious breach of security and may result in dismissal. The following is an indicative list of email related actions that are not allowed (the list is not exhaustive):

- Transmission of any personally identifiable or otherwise confidential information unless encrypted with approved encryption tools.
- The unauthorised transmission to a third party of confidential material concerning the activities of Standguide.
- Creation or transmission of material that brings Standguide into disrepute – either inappropriate or illegal use.
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind.
- The transmission of material that infringes the copyright of Standguide or another person, including intellectual property rights.
- Deliberately forging messages or creation or transmission of anonymous messages (i.e. without clear identification of the sender).
- Activities that violate the privacy of others or unfairly criticise or misrepresent, including copy distribution to other individuals.
- The deliberate unauthorised access to IT services and facilities.
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, or political or religious beliefs.
- Creation or transmission of any offensive, obscene or indecent images, message, data or other material.
- Creation or transmission of material that is designed to cause distress, inconvenience or anxiety.

(See appendix for examples of acceptable and unacceptable use)

Guidelines for Use

Inappropriate use of distribution lists wastes both network resources and staff time, for this reason they are to be used solely for business purposes for distributing mail which is relevant to everyone on the list.

All Email messages are recorded and can be presented as evidence in a court or tribunal.

Be careful what you write because you don't know where copies of your email message may end up (emails can be printed off or forwarded to limitless numbers of people). Inappropriate content of email could lead to problems for the sender or the organisation - bringing into question our professionalism and integrity.

If you receive, in error, a message meant for another person, you should on first realising that it is not meant for you, stop reading the message and return it to the sender, deleting any copies held. If the message contains confidential information, this must not be used or disclosed.

You can use email for a reasonable level of personal use. The following is considered to be unreasonable use; again, the list is not exhaustive:

- A level of use that is detrimental to an individual’s work performance.
- Any use of a commercial or profit-making nature, or for any other form of personal financial gain.
- Any uses that conflict with an employee's obligations to their employer.
- Use considered being against the organisation’s rules, regulations, policies and procedures - this email policy.

Limits and Quotas: All email accounts on the centrally managed server have quota limits placed on them, however limits are generous and should never be reached provided the following guidelines are adhered to (e.g. Staff are allocated a @standguide.co.uk address and an individual mailbox with 50 Gigabytes of storage space):

- Regularly delete unwanted email messages and the contents of ‘sent items’ and ‘deleted items’ folders.
- Copy any mail and/or attachments you need to keep to your “OneDrive” folder.
- Users will receive email notification when approaching their quota limit and are encouraged to follow the above guidance to manage their account.
- Once over quota no further email can be sent from an individual's account until they have reduced their storage to below the set limit.

Monitoring

Users should be aware that the nature of electronic mail makes it less private than they may anticipate - consequently the confidentiality of email cannot be assured. For example, an email message intended for one person may be forwarded to many others. Furthermore, even after a user deletes an email message from a computer or email account it may still exist on backup facilities. Standguide reserves the right to inspect, monitor, or disclose email messages, and may deny access to its email services:

- When required by and consistent with the law.
- When there is substantiated reason to believe that there has been a violation of the law or of the organisation’s policies.

The organisation will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves the organisation’s IT facilities.

Where there is evidence of an offence, the incident will be investigated and acted upon in accordance with the organisation's disciplinary procedures. In such cases Standguide reserves the right to disable accounts or block email to prevent further damage occurring.

8 Passwords

The settings for Standguide password policy are as follows:

- Password Length – Minimum 8 characters;
- They must contain at least one capital letter, one non alpha-numeric character within the eight characters.
- They must be easy enough to remember, to prevent needing to write them down and risk losing such information.
- Passwords must not be personal names or dates of birth.
- Passwords must not be password or any derivative of this.
- Password duration – 60 days (approx. every 2 months). If this is not enforceable a reminder will be issued to staff;
- Minimum password age – 0 days (this allows a user to change their password at any time, multiple times a day);
- Maximum password age – 60 days (0 days leeway);
- Enforce password history – 3 (users are not allowed to use the last 3 passwords);
- Number of unsuccessful login attempts – 5;
- Lockout duration – Locked out accounts need to be reset by the system administrators.

There will not be a complexity rule enforced (users have to use capital letters, lower case letters, numbers and special characters) until this has been reviewed thoroughly (as some systems may not accept complex passwords, although users are encouraged to make their passwords as strong as possible by using the complexity principles if they are able to. The following table will be used to show users what characters they should use in their password.

Group	Examples
Uppercase letters	A B C ……….
Lowercase letters	a b c ……………
Numerals	0 1 2 3 4 5 6 7 8 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /

Examples of bad passwords are:

standguide	-	There are no capital letters or non-alpha-numeric characters
Standguide	-	There are no non alpha-numeric characters
standgu!de	-	There are no capital letters
Stand#	-	There are not enough characters

Examples of strong passwords are:

!ndiGo99

Ch!caGo57

eleph@nT

boTT1ene<k

Please note: none of the above passwords should actually be used!

9 Support for Computers & Software

Depending on your office base, there are varying levels of IT support. In Head Office, the IT Infrastructure Manager usually receives and co-ordinates all requests for help. Time, resources and knowledge permitting, the IT Infrastructure Manager will try to resolve the problem. Failing this, a job will be logged with Axon-IT, with whom we hold a support contract and SLA (Service Level Agreement).

In offices that are supported by not support by Axon-IT, staff should report problems to the IT Infrastructure Manger via email or telephone. The IT Infrastructure Manager will arrange for the most appropriate support engineer to rectify the problem.

In offices that are supported by Axon-IT, the IT support is provided via a helpline telephone number 0845 313 0025 or email address support@axon-it.com. Axon-IT staff will log the request and initiate the appropriate action to rectify the problem.

Software applications supported are: Operating System, Applications support (MS Word, MS Excel, MS Power Point, MS Outlook and MS Access). Additional software system support may also be available (e.g. Microsoft SharePoint, Maytas) available from third party providers.

Training may be available to staff through Standguide negotiated courses or training sessions – you should ask your line manager if you feel you need additional training.

10Web Services

Standguide relies heavily on many web services: we publish material on the web and our staff and customers expect the content to be of high quality, well presented and easily available.

11Data Structures & Storage

All data is the property of Standguide. That includes data that is stored on Standguide fileservers, email servers and local machines under user’s personal directory. This also includes data that is held remotely on hosted systems (e.g. MAYTAS). Electronic communications (i.e. email messages) constitute part of the data. Thus, they are the property of Standguide.

Standguide data structure

Standguide maintains a shared drive structure that is used by Head Office staff for the storage and retrieval of corporate data.

Users of this structure must pay particular attention not to over-write or delete data that does not belong to them. This directory has structured with access to files restricted to only those users with a business requirement to access them. Users will be informed in advance of any further changes.

A document detailing the Head Office server directory structure and user access permissions is maintained by the IT Infrastructure Manager.

Individual accounts

Sufficient space is provided for Head Office Staff to store and retrieve data on the main file server in their personal folder (USERDATA folder).

This space is limited and it is the user’s responsibility to periodically transfer essential, old and unused files to CD for safe storage.

The storage capacity is provided for Standguide work and for reasonable personal use, for example, a letter you must type or to update your Curriculum Vitae. If you are not sure if work you intend doing is in breach of this policy, ask your line manager or contact the IT Infrastructure Manager for clarification.

All corporate data must be kept under Standguide directory structure (Z). Whilst you are working on a report, you can keep the files that you would like restricted to only yourself in your USERDATA folder. By saving the file in one of these locations, your file will be backed-up on the server.

Once the report is concluded, all the material (report, supporting files, graphs etc.) should be transferred to the appropriate Standguide shared directory to allow access to other users within your team. If restricted access is required, the file should be saved in a restricted sub-folder of the folder. If you require a restricted folder to be created send your request to the IT Infrastructure Manager along with the names of Staff who you wish to grant access to the folder.

12Security

Network security

The introduction of viruses when viewing websites, downloading software or other files from the internet poses a risk to each network on which we operate. Anti-virus software provides an element of protection but downloading also needs to be strictly controlled.

Individual computer firewalls should never be disabled. Should the installation of a software application require the modification of the local computer firewall the IT Infrastructure Manager should be consulted as this may require Administrator rights and will only be allowed providing no other problems with the firewall modification can be foreseen.

Generally speaking, downloading programme files should be disabled in Group Policy for normal users. These measures are generally managed by the IT Infrastructure Manager. If you require a programme or download, you should make sure that is necessary for you to perform your duties and ask your line manager to contact the IT Infrastructure Manager to arrange this under an administrator log-in and/or have the appropriate permissions configured.

At individual user level, security is generally provided by using passwords. This policy states clearly the rules which you have for the use of passwords, changing passwords and for not disclosing them (see section 8 for guidelines on passwords).

The use of autocomplete is discouraged as this can store passwords on your computer, which could be used by anyone who gains access to your machine. It has not been removed or prohibited as many people find this function important; however, you should be aware of the implications of using it and make sure you take all other steps to secure your workstation.

You must lock your workstation (by pressing Ctrl+Alt+Del) when you move away from your desk, to avoid people accessing not only files stored on your individual machine, but access to the internet, email and shared drives under your user profile. If inappropriate content is accessed or emails sent by that person it will reflect on you. The screensaver can be set to lock your machine when you are away from it. For help with this please see the IT Infrastructure Manager.

Care should be taken to avoid unauthorised viewing of information when in public places and the use of a password/screen-lock should be considered if you have any security fears.

You should be aware of people reading over your shoulder – not just when using a laptop on a train, but also in the office. If you work on sensitive information and require a screen privacy protector you should make your case to your line manager who will approach the IT Infrastructure Manager (a privacy protector will not allow people to view your screen unless directly in front of it).

You are bound by your contract of employment and by the organisation’s confidentiality, intellectual property and data protection policies with regard to the information you come across in the course of your work. You may not disclose information relating to any identifiable individual, either customer (e.g. event delegate or course participant) or staff. Additionally, you may not disclose confidential information relating to any aspect of the business of the organisation. Internet users must be aware that the system is inherently insecure. No personal information or other information that is confidential to the organisation must be transmitted over the internet unless encrypted with approved software.

Encryption

All the physical controls on security, and the use of security level logons, are negated if information transmitted via the internet and email is intercepted along the way. Emails are extremely easy to intercept, and so the key consideration for transmitting information has got to be that an assumption is made that it will be intercepted, with the emphasis being that any information within an email is encrypted in such a way to make it meaningless to an interceptor.

Standguide will be adopting a minimum level of encryption security, as a minimum meeting the requirements of Level 1 of FIPS 140-2 (a Federal Information Processing Standard used to accredit cryptographic modules). Standguide are committed to encrypting all full hard drives used for the processing and storage of confidential information to the FIPS 140-2 standard or higher using Disk Protect or similar software.

USB Memory Sticks

All Standguide staff will be provided with an encrypted memory stick for the storage of files. Approved memory sticks are hardware encrypted using 256bit AES encryption and FIPS certified. No other memory sticks may be used. Staff found using non approved memory sticks may be subject to disciplinary proceedings.

Security Breaches

Recording security breaches enables the organisation to improve the quality of service. In line with section 9 of the Standguide Information Security Policy, you are encouraged to report incidents for this purpose:

- Any security breaches (or suspected breach) must be reported, either directly or through your line manager, to the IT Infrastructure Manager who will investigate the matter.

Security of portable (notebook/laptop) computers

Portable computers present a higher risk in terms of:

- Theft – Bear in mind that it is not only the computer that it is at risk; more importantly, it is you that risk being injured if an attempt is made to steal your notebook computer, or if you attempt to prevent it being stolen (i.e. by a mugger).

- Data – Care should be taken to avoid unauthorised viewing of information when in public places and the use of a password/screen-lock should always be used. Likewise, printouts of electronic data should be protected – making personal information anonymous, etc. Under no circumstances should contact details or any files containing personal information of customers (clients) be held on laptops.

- Under no circumstances should users copy entire folders or directories to their laptops – this potentially represents a massive data loss. Only several files should be copied to the laptop at any one time and these should be needed in order to work offline. Any more than a few files should be held on an encrypted memory stick – these are available from the IT Infrastructure Manager. However, one should still try to keep offline storage (files not held on the organisation’s shared drives) to a minimum as this may cause problems with version control and backups.

- Under no circumstances should users copy or store any organisational data on personal hardware (e.g. home computers or hard disk drives). All work done on behalf of Standguide belongs to the organisation and should be stored on the corporate system or Standguide provided equipment under the above rules.

Office Security

General office security is very important to computer security for a number of reasons. End of day procedures that are important include:

- Ensuring that equipment is shut down and turned off (including monitors) reduces the problem of unauthorised people gaining access to our systems, as well as reducing power costs and the associated effect on the environment.

- Any printed material should not be left in the printer tray. If you are printing confidential documents, ensure that you collect these immediately. If the printout does not appear check the computers printer queue. If you suspect that a confidential printout has gone astray, you should inform the IT Infrastructure Manager or your Line Manager immediately. Where possible try to anonymise confidential material for printing.

- Laptops that are left in the office should be locked in a drawer overnight, as using a laptop lock would not be much of a deterrent to a thief in this scenario – you could probably only lock it to the leg of the desk (which could be lifted to remove the lock) or the monitor (which could probably be unscrewed or broken or stolen as well).

- Make sure that all windows are closed – if you open a window; make sure you close it before you leave or that someone else will close it for you.

- FAX security – Try to limit the use of FAX as a communication means, but if this is required, ensure that you telephone the recipient prior to sending the fax so that they can be at their fax machine to personally receive the transmission.

Outside Security

Other security measures should be observed whilst out of the office:

- Lock laptops in the boot of your car and not in plain sight – as well as protecting your personal safety, vehicle and our equipment, you may find that insurance policies will not cover this type of theft.

- Be aware of your surroundings – do not view personal information or documents that are sensitive to the organisation in public, where someone could read over your shoulder (e.g. using a laptop on a train).

- Do not ‘flash’ your equipment (laptops, mobile phones, etc.) to avoid being mugged. Always be aware of your surroundings and your personal safety.

- In the event of loss (but not theft) of any IT equipment, you may be charged for a replacement.

- Printouts of personal or delicate information should, where possible, be made anonymous.

13Important Links & Other Useful Literature

http://www.england-legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm - The Computer Misuse Act 1990

http://www.opsi.gov.uk/acts/acts1998/19980029.htm - The Data Protection Act 1998

http://www.ico.gov.uk – The Information Commissioner's Website

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_3 - The Human Rights Act 1998

Monitoring Arrangements

The policy will be managed by the Quality Assurance Manager and IT / Infrastructure Manager as a result of cross company meetings. All meetings feed into the Senior Management Team Meetings. The Senior Management Team has overall responsibility for creating an ethos and environment that reflects the policy

Review Procedures

The Senior Management Team will ratify the policy.

Review Date: **October 2021**

14Appendices

Email

All users are allocated a @standguide.co.uk address. This email address is primarily for **business use,** i.e. for use relating to the work of Standguide; however, as we have already stated, some personal use is acceptable as long as this does not contravene the unacceptable usage stated in the policy.

An example of what is acceptable:

Sending and receiving brief emails to friends and family or colleagues on the proviso that any attachments you send have been checked for viruses and are deemed safe. Please use common sense when determining what others may find offensive and err on the side of caution. (Likewise, if you receive an email that contains any material that may be deemed offensive or inappropriate, delete it immediately and do not forward it to other users. If you receive this email from outside the organisation, please inform the sender that it is not acceptable to send such content to your work email address.)

An example of what is not acceptable:

Using your work email address to receive non-business related email circulars e.g. from holiday companies, supermarkets, shopping websites etc. which use up valuable storage space and create a huge volume of traffic on our email servers. Email should not be used as a chat/instant messaging service. A personal email address should be used for signing up to receive non-work emails; if you use a web-based service such as Hotmail or Google mail, you can access email from home or work (within reason) and these services provide far more storage space for your emails of choice. If anyone doesn't have a personal email account, please let a member of the IT Premises team know and we'll help you set one up. As with work emails, these personal emails should not be used excessively during working hours.

As space is limited please remember to regularly delete mail you no longer need or place it in your archive. A help file is available explaining how to set up and use an archive - please ask a member of the IT Premises team for help with this if necessary.

Internet

As with work email, the internet is provided as a business tool for gathering information. Personal use of the internet is acceptable within reason as long as this does not contravene the unacceptable usage stated in the policy.

An example of what is acceptable:

- Spending five minutes checking your bank account details, personal email or carrying out quick information searches during the working day.

- Browsing the internet to look at, for example, houses for sale, online retail sites or car insurance quotes for the duration of your lunch break or during other defined break time.

- Browsing the internet before starting work or after your working day has finished.

Examples of unacceptable use of the Internet:

- Visiting internet sites that contain obscene, hateful, pornographic, extremist, terrorist or otherwise illegal material

- Using a computer to perpetrate any form of fraud, or software, film or music piracy

- Using the internet to send offensive or harassing material to other users

- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license

- Hacking into unauthorized areas

- Publishing defamatory and / or knowingly false material about Standguide Ltd, your colleagues and / or our customers on social networking sites, blogs, wikis or other online publishing sites.

- Revealing confidential information about Standguide Ltd. in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and / or internal discussions

- Undertaking deliberate activities that waste staff effort or networked resources

- Introducing any form of malicious software into the corporate network

- Anything which significantly impacts on your working time, for example: Spending 25-minute sessions browsing the internet or playing online games during the working day outside break times.

Messaging / social networking sites

It is not acceptable to use social networking sites (e.g. Facebook) at work. You should not use personal instant messaging (e.g. MSN Messenger) and should not be installed on the organisation's computers. We provide a messaging tool for business use, and this should be utilised for all business related instant messaging communications, as it is monitored for your safety.

Definition of the IT Premises Team

The IT Premises team is responsible for all aspects of the Standguide computer network and telephony infrastructure as well as all computer systems connected to the network and the implementation and adherence to IT Security requirements.

NB. Please be aware that this policy is subject to change. Any future changes will be made known or available to staff as soon as they are approved by the Senior Management Team. However, you will not be required to sign off on these changes as you are already aware of a policy covering the use of computer equipment.

This policy is non-exhaustive and if something is not written or discussed in this document then users should consult the IT Infrastructure Manager before making IT related decisions – e.g. using programmes, making data backups, requesting configuration changes to equipment, etc.

Monitoring Arrangements

The policy and associated procedure will be managed by the IT and Infrastructure / Quality Assurance departments as a result of cross company meetings. All meetings feed into the Senior Management Team. The Senior Management Team has overall responsibility for creating an ethos and environment that reflects the policy.

Review Procedures

The Senior Management Team will ratify the policy.

Review Date: October 2021