Information and Communications Technology Policy

Nov 2019

Version 1.3

Statement of Intent

This policy document is written to:

- outline some responsibilities of the IT staff in providing ICT infrastructure
- aid other staff members to understand ways in which the ICT system is and isn't allowed to be used
- aid in the maintenance of security, integrity and performance of the company's computer systems
- minimise legal risks associated with the ICT systems and their use

Scope

The policies outlined in this document apply to all staff members and to any users of ICT infrastructure used throughout Impamark. Comments and queries regarding this policy document should be given to the IT department or management of the company.

Ownership

Information transmitted via the Impamark network is owned by Impamark. Impamark retains rights to the information and has the right to open and view such information at its discretion. Impamark may retain information for a period deemed fit by Impamark. Information can come through multiple sources and include, but is not limited to, such things as:

- network traffic
- documents, files etc.
- email

Employees' liabilities

Failure to comply with policies outlined in this document may result in disciplinary action, a removal of system privileges and even dismissal from Impamark.

Some ways of misusing the ICT systems may leave employees liable to legal issues.

Please note, you have been warned

Computers and Associated Hardware and Software

Impamark provides access to a computer and appropriate software for each employee. Use of email and the internet is for business purposes only. Employees may need to, at some point, use a computer for personal matters. This is only acceptable in an emergency, or when necessary and authorised by your manager.

Home Computers

Computers from home are not under the administrative control of the company and would not generally be supported by the IT department. The connections of home computers to the company network is prohibited unless authorised by the IT department.

Confidential data from the company should not be stored on home computers. Confidential data includes, but is not limited to, financial information and personal information the company handles. Confidential data should be handled in accordance with the General Data Protection Regulation (GDPR) and any other relevant laws and regulations.

With proper authorisation it may be possible for staff to work from home. This is at the discretion of the company. In cases where a member of staff is working from home, the IT department must be consulted beforehand. Electronic equipment used during the course of work must comply with company standards. Phones can be set up to allow phone calls more easily between external staff and the company. Additionally it would be possible to allow access to the company file-server. The company may choose to supply equipment rather than have staff use their own possessions.

Passwords

Passwords are mandatory for access to our system to prevent unauthorised access

Password security

Passwords should be committed to memory and not written down unless put in the safe over night. For security reasons, work passwords should never be used outside of the office. If users need a password for subscription to an external site then the IT department should be contacted for advice.

Password Strength

All passwords provided by the IT department should generally be a minimum of 8 characters containing at least one of each of the following:

- upper case letter
- lower case letter
- numeral
- one other character

Generally passwords are provided by the IT department and are the same for each user across different services controlled by the company.

When creating passwords it is often better to have one of a greater length even if it appears less complex. For example ‘SonyBotanicalsGlassvistaBush1#’ is better than ‘A8#%’. Staff can speak to the IT department for information.

Users should not divulge their passwords to anyone else, particularly to people who are not part of the company. Individuals may be liable for actions conducted under their username or password.

Internet Usage

Monitoring and logging

Please note that all internet usage is logged and may be monitored at any time. IT staff can see when computers are uploading and downloading data. Additionally the company logs and monitors all data passing through its system. Network logs are made automatically and are used for fault diagnosis and performance troubleshooting.

For business purposes only

The company provides IT infrastructure for business purposes only. The use of the internet is no different and should only be used for business purposes.

A privilege – not a right

Whilst the use of internet and email is an integral part of the company’s work-flow, internet access is not a right. This privilege may be removed at the discretion of the company.

Discretion

Impamark retains discretion over what constitutes legitimate business use and what is illegitimate and misuse of the IT infrastructure.

Internet access levels

Use of the internet is divided up into only two access levels, as follows:

- No access – All access to the internet and outside services is barred. Local network access is allowed for accessing the file server. Use of phones or instant messaging (i.e. Rocketchat) may be allowed to allow communication with the Spanish office.
- General unlimited access – Impamark does not limit access staff have to network. Impamark does not block any websites and staff are trusted to use IT infrastructure appropriately.

Wi-Fi

Along with wired internet access, Impamark also has wireless internet access available. As with wired internet access, the Wi-Fi should not be used for personal use during work hours.

In the UK office there are two different Wi-Fi connections available, 'TEST' and 'General'. TEST is for internal use only – that is for use by staff. 'General', like the name would suggest, is for general use (for example for those external to the company i.e. visitors). While the password for General is more likely to change than the one for TEST, either may be changed at the discretion of the IT department. Please consult the IT department if the password is required.

Email

Emails are one of the two primary sources of communication at Impamark. Email has its benefits but can also be a great time waster.

Security - viruses

One of the largest threats to the company are viruses and other malware in emails. The best virus checker is actually the user.

The company does run a variety of systems to block emails containing viruses plus spam/junk. None of it is perfect and a trained user is better at spotting junk and viruses than a computer.

Do NOT open attachments received unless you are absolutely sure of their origin. Often emails can look extremely convincing. Check and double check. One minute of your time checking carefully could save the company hours of wasted time recovering from an infection.

Often these attachments use an archive file format (such as zip, 7z, and RAR) or an executable format (such as an exe or deb). Attachments in these formats should be distrusted and, unless authorised, not opened.

If in doubt ASK the IT Department for assistance

Internet Mail Systems

Email accounts are set up and maintained in the company internal systems. Accounts with external Internet Service Providers (ISPs), or stand-alone email providers, should not be set up.

Email Software

Currently Mozilla Thunderbird is used to send and receive emails. Additionally our CRM, vTiger, can be used to send emails.

Plain Text and HTML email

In order to embed images and graphics within the body of an email, many companies use HTML email. Although attractive it can lead to issues with legibility. For most emails Impamark prefers the use of plain text as it can be read easily on any device.

Encryption and signing

A ‘signed’ email verifies that the person purported to have sent the email actually sent it. Encrypting an email ensures that only those meant to read message can.

Impamark currently uses Enigmail for OpenPGP support. This allows emails between members of staff and clients to be signed, encrypted, or both signed and encrypted. The IT department will generate encryption keys where appropriate. They should not be altered in anyway, or used for personal communications.

Email Addresses

Email addresses must conform to a company address standard. This means that users’ email addresses conform to username@impamark.co.uk where the username is usually the user’s first name. Some general addresses exist such as info@impamark.co.uk which forwards all emails received to multiple people.

The company has a backup Gmail account, sovereign.insignia@gmail.com. It can be used if staff are having trouble with sending or receiving emails to or from a particular person. If emails are bouncing the IT department should be consulted. Emails sent to this account may be read but the account should not be used to send emails unless authorised.

User Obligations

Users provided with email have an obligation to read emails received, and if necessary respond in a timely fashion. Not all emails and instant messages may require an immediate response. A balance should be struck between a timely response and limiting the interruption of a staff member’s normal work-flow.

It is customer policy that, if possible, customers should be quoted within 24 hours. In cases where it isn't possible (say for example a customer makes contact at the end of the day on a Friday), customers should be quoted as soon as is possible.

Staff should not subscribe to email services for the purpose of sending or receiving inappropriate material including material which is offensive, pornographic, or creating an unnecessary burden on the network. Users are obligated to not send inappropriate or offensive emails as they reflect on the company and may bring it into disrepute. Users should not represent their opinions as those of the company.

Email Privacy

The company is at liberty to read any employee emails at any time without notice.

Email Personal Use

Email is strictly for company use only. Emails should not be used for personal private matters.

Footer

Users should have an email signature of a form similar to:

```
Person Name - Job Role
+44 (0)1621 783550

Please consider the environment before printing this email
Only print if necessary, and where appropriate only those pages required
www.facebook.com/ImpamarkPBM
www.impamark-promotional-merchandise.co.uk
www.regimentalmerchandise.co.uk
www.impamark-promotional-merchandise.co.uk/blog
www.twitter.com/Impamark

Officially Licensed by the MOD and Suppliers to HM Forces
Member of the British Promotional Merchandise Association

2017 Top 25 Winner - Distributor of the year Awards
2014 Top 25 Winner - Distributor of the year Awards
2012 James Norman Award for services to the Envoy Group
2009 Celebrated 40 years as a family run business
2008 Finalist of the Essex County Business Awards
         Business to Business Category
2007 Winner of the Mid Essex Business Awards
         Business to Business Category

Sovereign Insignia Limited T/A Impamark
```

```
1 Dammerwick Farm, Marsh Road, Burnham on Crouch, Essex, CM0 8NB
Tel 01621 783550 Fax 01621 784548
```

The IT department will implement this for users and it should not be altered without prior authorisation.

Attachments

Due to the nature of our business we receive many large attachments such as artwork. Note that very large attachments are automatically blocked from being received so it does not impact network performance.

Large files should not be sent as attachments to an email as it can have a negative impact on network performance and may not be received by some people. Some customers, such as councils, limit the size of attachments which can be received.

If a large file is needed to be sent or received we have a number of other methods that can be employed. The simplest is a plugin to Thunderbird called DL. To send an attachment you can attach the file and then convert it to a DL attachment which embeds a clickable link in your email. To receive a large attachment you can send the client a DL 'grant' where they can upload the file directly to our server and we can then download at our convenience or send the link to a supplier.

EPS files (used for vector artwork) should not be sent to customers as customers are unlikely to be able to open and view them. Instead please, when sending artwork to customers, export EPS artwork as a PDF. EPS files should only be sent to suppliers.

Folders and Filtering

Email filtering can be used to automatically move emails to certain folders in Thunderbird. Please consult the IT department if this is desired.

Impamark however encourages that staff limit the use of folders and sub-folders. With many customers the number of folders can easily become excessive. Too many folders and sub-folders can make it harder for staff to find emails (especially staff who are looking through another staff-member’s emails).

Thunderbird also includes an alternative to folders, which can be less messy, which is email tags. Emails can be tagged to be under a particular category and colour-coded. This can make searching easier.

Web Browsing

Web browsers are one of the primary tools used in the company.

Personal Usage

The use of web browsers for personal reasons during work hours is not permitted unless authorised or in an emergency. This includes the accessing of personal email and the use of personal social media accounts.

Advert Blocking Software

Impamark uses software to block advertising on web-pages. This software is a web browser extension for both Mozilla Firefox and Google Chrome known as Ublock Origin. While doing little else than blocking advertising there is the potential that it could affect the usability of certain sites. Please consult with the IT department if needed.

Safe Browsing

Staff should be wary of unknown websites. Some websites may cause the downloading of malicious software which could compromise the system. Software from outside the company should not be run without proper authorisation.

Web sites which use HTTPS instead of HTTP are preferred as they are more secure. HTTPS adds a layer of encryption which prevents third parties tampering with the contents of a site in-transit. Both Chrome and Firefox indicate that a website uses HTTPS with a green padlock graphic.

Instant messaging

In order to help coordinate the UK and Spanish offices we use both phones and Instant Messaging. Instant Messaging has the benefit of keeping a record of conversations for later reference.

RocketChat

Rocketchat was introduced to replace the company’s use of Skype. It is used to send messages between individual staff members, to multiple staff members at once, and to make video-calls. Generally it is for employee conversations only but it is possible that customers could be added if required. Please contact the IT Department accordingly.

The server-side software is controlled by Impamark. In order to use Rocketchat client software can be used or employees can log-in via a web browser via https://chat.impamark.co.uk

Skype

We no longer use Skype for communications. However we do maintain some Skype accounts for customer contact as required. If you require a Skype account for work please contact the IT department. Personal Skype accounts, or adding personal contacts to a work account, are not

permitted.

Phones

Phones are an important tool and an integral part of Impamark’s working procedure.

Desk Phones

Each desk is currently supplied with two phones. One is a Mitel IP phone and the other is a Telrad phone. The Telrad phones will be phased out so only IP phones will be used eventually.

Telrad – 01621 783550

This is the main phone with four incoming/outgoing lines

Mitel/Grandstream – 01621 834980

This is a test SIP system with two incoming/outgoing lines

Every phone is capable of ringing any UK number, ringing anyone within the UK office, and ringing out to Spain to the Spanish office.

Certain numbers may have restricted usage e.g. higher rate numbers or inappropriate services.

The phones are available as a business tool and private calls are not permitted without authorisation.

Mobile Phones

Mobile phones should not be used during working hours, unless the use of mobile phones is a necessary component of a staff member’s job or prior authorisation is obtained.

Use during Working hours

The use of personal mobile phones in the workplace is not allowed during working hours. This includes text messages and all mobile messaging including Facebook, Whatsapp etc. However, you may use your mobile phone during your normal contractual break periods.

All mobile phones must be on silent at all times whilst working. Failure to do this may lead to disciplinary action being taken.

Sales staff at an event would be permitted to use their phones to contact the company, at an event for example. Similarly, IT staff would be permitted to use mobile phones in maintenance of company infrastructure.

Charging

To prevent the spread of malware to the company networks employees should not use USB cables to connect their phones to computers for charging purposes.

The use of USB cables for charging is not permitted unless an adapter is used so that it draws power using a mains plug. Employees may charge mobile phones using a charger at the wall. Spare USB to mains plug adaptors may be available for use.

Software

We use a large variety of Open Source software on our systems. N.B. Windows programs will NOT work on Linux desktops. Please do not try and install them.

Installation

Under normal operating procedures, IT staff will be responsible for the installation of software onto desktop and laptop computers. Normally users are trusted to install updates. If software beyond the standard installed applications is required. The standard set of software used by the company may change at any time at the discretion of the company.

Staff should not download or install software from outside sources.

Intellectual Property

Code which is written in-house is to remain the intellectual property of the company, Impamark. The copyright concerning bespoke software written by outside individuals will be worked out on a case-by-case contractual basis.

External Hardware Usage

External hardware may bring viruses or malware that can contaminate company systems and cost the company time and money to rectify.

Usage

For security reasons there shall be limits on the usage of hardware not provided by the company. External devices should not be connected to company computers or equipment. This includes (but is not limited to) external storage devices such as USB flash drives, memory cards (i.e. SD cards and Compact Flash), external hard-drives, optical discs, and media players.

To facilitate this policy the IT staff may take measures to prevent external USB devices from being mounted (to mount a device is to connect it and have its files accessible to the computer system).

Backups

To protect the company we run a variety of backup systems.

Regular copies of the databases and other data are made. If there is a failure in the IT infrastructure, the IT department will restore data from a previous backup but some data may potentially be lost.

RAID Systems

Each server makes use of RAID technology. RAID stands for ‘Redundant Array of Independent Disks’ and is where multiple hard-drives are used to create one fault-tolerant storage system. This is a first layer of protection against hardware failure.

Replication

Data stored on the main server is replicated throughout the day to the server in the Spanish office. There is also a dedicated backup server upstairs.

Off-site backups

Regular (daily) backups are made to one of two portable hard-drives downstairs. Each day a drive will be taken away from the office in case of a disaster. The next day the drive taken will be swapped with the drive in use.

File storage

All data should be stored in the company server and not on local computers. Files stored on computers locally will not be backed up and may be lost in the event that the local machine has a failure.

Media Statements

Please refer all press or media enquires to Nicola Crisp, the Managing Director. Staff should not organise, hold meetings or make contact with the press or media (traditional or online) individually. If someone from the media makes contact for any reason please refer them to the managing director.

Personal Social Media

While employed by Impamark, staff should not write material on personal social media that may bring the company into disrepute. This may be grounds for dismissal.

Use of Surveillance Cameras

The company may use surveillance cameras for safety and security reasons.

- The employee should be aware that they may be monitored while working for the company
- The employee consents to the collection of information in this way

The company will abide by the relevant laws including the provisions of the Data Protection Act 1998 and GDPR when collecting and storing such information.

Webcams may be fitted and used for communication. They are not used to surveil staff.

Treatment of Confidential Information

Information about customers is personal data and should be treated with care. Under the Data Protection Act 1998, staff are legally obligated to keep customer's personal data confidential. The same is true under the GDPR (General Data Protection Regulation).

Data should not be transferred outside of the European Economic Area. Personal data is defined legally as "data which relate to a living individual who can be identified" from the data or data likely to be in possession of who is in control of the data.

Customer information should not be transferred outside of the company. It should not be distributed, disclosed or disseminated in any manner. Employees should not use customer information except for purposes for which they have been authorised.

Financial information should also be treated as confidential and may not be disseminated freely.

Signed by User: Signature:

Date: / /

Signed by Manager: Signature:

Date: / /