garden organic

IT and Information Security Policy

2017

IT and Information Security Policy

Supporting policies

- Data Protection policy
- CCTV policy
- Code of Professional standards (Employee Handbook)
- Disciplinary policy (Employee Handbook)

Aims of the policy

Whilst the Organisation encourages embracing IT to its fullest extent to help individuals work at their most effective capacity it is important that guidelines are issued for the protection of the individual and the Organisation. The objective of this policy is to ensure all users of the Organisation's IT facilities do not unintentionally place themselves or the Organisation at risk by carrying out computer related activities that contravene this policy.

Scope

The scope of this policy includes all users who have access to computers owned by the Organisation and/or its network/systems or those who access the Organisation's network/systems via personally owned devices. It also covers private use of social media.

This policy applies not only to employees but also to volunteers, trustees, associates, service users, beneficiaries and anyone else requiring access to the Organisation's network and systems including the Organisation's IT contractor. These individuals/groups will hereafter be referred to as 'users' or 'affiliates'.

Public access to the Organisation's externally reachable systems such as the charity's website or the on-site public Wi-Fi at head office is specifically excluded from this policy.

Principles

The Organisation demands respect from all employees and volunteers, its customers, partners, the wider community and for each other. This means systems must not be used in a detrimental or offensive way.

The Organisation demands integrity from all IT users so that it is confident that the Organisation is not and cannot be accused of facilitating any unlawful or offensive action at any time.

The Organisation expects commitment to ensure it is seen as exemplar in the way it conducts its business which includes the way it uses its IT systems.

The Organisation respects the individual privacy of its IT users. However privacy does not just extend to work related activities or to the use of Organisation provided equipment. IT users should be aware this policy might affect privacy in the workplace.

In the event of a breach of this policy users may face disciplinary action (or other sanctions deemed appropriate to their association with the Organisation) if they breach this policy and/or bring embarrassment on the Organisation or bring it into disrepute.

Legislation

All users shall comply with the relevant legislation. This includes the following:

Data Protection Act 1998/Freedom of Information Act 2000 - any information which the Organisation holds is potentially disclosable to a requester under one of these pieces of legislation. This includes emails too.

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

- passing on personal information about an individual or third party without their consent;
- keeping personal information longer than necessary;
- sending personal information to a country outside the EEA.

Computer Misuse Act 1990 - this Act makes it an offence to try and access any computer system for which authorisation has not been given.

Copyright Design and Patents Act 1988 - under this Act it is an offence to copy software without the permission of the owner of the copyright.

Defamation Act 2013 - under this Act it is an offence to publish untrue statements which are likely to cause serious harm to the reputation of a person, a group of persons or a body that trades for profit.

Counter Terrorism and Security Act 2015 - this Act makes it a criminal offence to encourage terrorism and/or disseminate terrorist publications.

Telecommunications (Lawful Business Practice) (Interception of Communications)

Regulations 2000 - this allows any organisation to monitor or record communications (telephone, internet, email, and fax) for defined business related purposes.

Introduction

Proprietary information contained on electronic and computing devices, whether those devices are owned by the Organisation or by an affiliate, remains the sole property of the Organisation. All IT users must ensure that any proprietary information is protected in accordance with the Data Protection Act (further information can be found in the Organisation's data protection policy).

IT users have a responsibility to promptly report the theft, loss or unauthorised disclosure of any proprietary information.

IT users are personally responsible for using good judgement regarding the reasonableness of personal use.

For network maintenance and security purposes, authorised individuals may monitor systems, equipment and network traffic at any time.

Safeguarding

Any users that interact with children/young people and adults at risk who are making use of the Organisation's IT must also refer to the Organisation's e-safety policy to ensure adequate protection is being given.

Access to the Organisation's systems/network

All employees/users who require access to the Organisation's systems/network must return a signed copy of this IT policy to confirm it has been read and understood before access will be granted. The IT agreement will either be posted to new employees/users as part of their starter pack or handed over on their first day.

Acceptable Use

The following activities **are prohibited** and the Organisation's network may not be used directly or indirectly for viewing, downloading, creating, manipulating, transmitting, forwarding or storing of:

- material that is offensive, indecent or obscene;
- material that is defamatory, discriminatory, threatening or extremist;
- material which is used to facilitate harassment, bullying and/or victimisation;
- unsolicited 'nuisance' emails;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party;
- any other material that brings the Organisation into disrepute.

Users should not:

- attempt to gain unauthorised access to restricted areas of the Organisation's network;
- access or attempt to access data where the user knows or ought to know that they should have no access;
- undertake any hacking activities;
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

Only employees/affiliates of the Organisation should be using Organisation equipment, it is not to be used by family members or friends.

Equipment owned by the Organisation must not be used for personal work, games etc.

System and network activities

The following activities are strictly prohibited:

- violations of copyright, trade secret, patent or other intellectual property including (but not limited to) installing or distributing 'pirated' software products or any other products that are not appropriately licensed for use by the Organisation;

- unauthorised copying of copyrighted material including but not limited to digitisation and distribution of photographs from books, magazines or other copyrighted sources, copyrighted music and the installation of any copyrighted software for which the Organisation or end user does not have a license;
- accessing data, an account or server for any other purpose other than for conducting business on behalf of the Organisation;
- revealing account passwords or allowing use of your account by fellow employees or anyone outside the Organisation including family/other household members whether working in the office or when working from home;
- providing information about, or lists of employees to anyone outside of the Organisation.

Internet Usage

Users are responsible for their actions when using the Internet and must ensure they do not undertake any activities which may bring the Organisation into disrepute as detailed in the acceptable use section of this policy. Usage of the internet for personal use is only permitted outside normal working hours e.g. lunchtimes or break times.

Access to the following categories of website will be blocked:

- gambling and gaming;
- pornography or other adult content;
- violence/racial hatred/radicalization and extremism;
- personal webmail accounts such as Hotmail/Gmail;
- freeware/software downloads;
- drugs/illegal drugs.

Users are expected to use the internet sensibly e.g. where it would be quicker to make a telephone call than to engage in an internet search for the required information then the telephone call should be made.

When using the internet the Organisation supports the following browsers: Microsoft Internet Explorer, Microsoft Edge, Google Chrome and Mozilla Firefox. Other browsers can be used but IT will not necessarily support these in the event of a user finding an issue in relation to their work.

There may be many sites that could be useful for the purposes of an employees/affiliates day to day work. Employees/affiliates wishing to register as a user of a website for work purposes are permitted to do so although users are encouraged to be cautious and consider the validity of the site before doing so. If in doubt users should check with their line manager before registering.

Users should not under any circumstances download software onto the Organisation's systems, it can only be done by the IT contractor. This includes software and shareware available for free on the internet. If users receive any software, demonstration or otherwise that they would like to make use of, it must be passed to the Organisation's IT contractor for their appraisal, documentation and, with consent from a head of department, installation.

Users must not move or copy software between computers. If software is needed on a particular device please contact the Organisation's IT contractor.

All machines have an anti-virus programme installed; this must never be disabled or removed by users. Procedures for guarding against viruses are the use of Firewall security and anti-virus and anti-malware products which are continually kept up to date.

The Organisation reserves the right to monitor internet usage and users may be called upon to justify the amount of time they have spent on the internet or the sites they have visited. The Organisation will endeavour to inform an affected user when this is to happen and the reasons for it. Access or monitoring of internet usage can only take place with the prior consent of an executive director.

Possible reasons to monitor internet usage may include, but are not limited to:

- if the Organisation suspects the user has been viewing/downloading offensive or illegal material;
- if the Organisation suspects a user has been excessively using the internet for personal use;
- if the Organisation suspects the user is making use of the internet in a way that is detrimental to individuals or the Organisation.

The Organisation reserves the right to restrict or deny internet access to any user at work, although in such a case it will endeavour to give a reason for doing so. Further, any inappropriate or excessive use during working hours may also be dealt with under the Organisation's disciplinary policy.

The Organisation's website

Only those who have been given express permission by the Head of Membership and Marketing may add and/or delete information on the Organisation's website.

Email usage

The Organisation provides access to email for business purposes although understands that users may on occasion need to send or receive personal emails using their work address. Users must always use their Garden Organic email address when conducting work on behalf of the Organisation. Use of personal email for business purposes is strictly prohibited.

Users are notified that communications made and received from a work address are not confidential so should not transmit messages that you wouldn't want read by a third party.

When using email or other communication vehicles users must not participate in any prohibited activities as detailed in the acceptable use section of this policy.

In addition, the following are strictly prohibited:

- sending unsolicited emails including junk mail or other advertising content to anyone who did not specifically request such material i.e. email spam;

- any form of harassment via email or telephone whether this is via content, frequency or size of message;
- unauthorised use or forging of email header information;
- creating or forwarding of chain letters;
- use of Organisational resources to access private webmail accounts such as Gmail or Hotmail (other than the dummy Gmail accounts set up on the Organisation's mobile phones).

All users should ensure email communications are in the correct house style (i.e. font and size) and have the correct auto signatures set up so that this is included on all email communication. Information on the correct house style and auto signature content can be found at F:\Staff General\Branding and Logos\Standard email signature.docx or alternatively please refer to the marketing department.

Emails that users intend to send should be carefully checked. Emails should be given the same care as all other forms of communication and, as such, what is normally unacceptable in a letter is equally unacceptable in an email. Users should ask themselves before sending an email how they would feel if their email were to be read out in Court as email messages may have to be disclosed in any litigation.

Statements that must be avoided in emails, both those sent internally and externally, include statements that criticise any of the Organisation's partners/affiliates or their employees or emails stating that anyone is incompetent. This is defamatory activity.

Users should take the same care when sending personal emails from their work address as sending work related emails.

Users should be cautious when using the 'cc' facility and take care not to copy emails automatically to all those copied into the original message as doing so may result in accidental disclosure of confidential information.

Users should reply promptly to all email messages requiring a reply. Where a prompt detailed response is not possible a short email acknowledging receipt and giving an estimate of when a detailed response will be sent should be sent.

Users should endeavour to keep their mail box tidy by deleting emails and saving attachments from emails to either the F or P drive.

Users should not create email congestion by sending trivial messages or by copying emails to those who do not need to see them.

The Organisation has good practice guidelines for dealing with email when employees/users are out of the office. When activating the "out of office" facility, messages should name an alternative employee/user for correspondents to contact if necessary and provide the switchboard contact number. This will ensure that any important messages are picked up and dealt with within required timescales.

The Organisation reserves the right to monitor users' emails but will endeavour to inform an affected user when this is to happen and the reasons for it. Access or monitoring of email accounts can only take place with the prior consent of an executive director.

Possible reasons to monitor email may include, but are not limited to:

- if an employee/user is absent for any reason and communications need to be checked in order to ensure the smooth running of the Organisation;
- if the Organisation suspects a user has been viewing or sending offensive or illegal material (although the Organisation understands that it is possible for employees to inadvertently receive such material and they will have the opportunity to explain if this is the case);
- if the Organisation suspects use of the email system for personal use is excessive;
- if the Organisation suspects the user is sending or receiving emails that are detrimental in anyway either to individuals or the Organisation.

When monitoring emails the Organisation will, except in exceptional circumstances, limit itself to looking at the address and heading of emails.

Users who receive improper email from individuals inside or outside the Organisation should discuss the matter in the first instance with their line manager or supervisor.

The Organisation provides a current and up to date automatic virus checker on all networked computers. The Organisation's email system operates a SPAM filter service that will quarantine junk email. The user is alerted to such email and has the ability to release the mail if they're confident it isn't junk. However, caution should always be used when opening any attachments or emails from unknown senders even if it hasn't been picked up by the SPAM filter. If in any doubt, always refer to the Organisation's IT contractor prior to opening any emails or attachments.

Inappropriate or excessive use of email may be dealt with under the Organisation's disciplinary policy.

Social media

Social media can bring significant benefits to the Organisation, particularly for building relationships with current and potential customers. However, it's important that those who use social media within the Organisation do so in a way that enhances the Organisation's prospects.

Social media sites and services include (but are not limited to):

- popular social networks like Twitter and Facebook;
- photographic social networks like Flickr and Instagram;
- professional social networks like LinkedIn and Sunzu;
- blogging.

Key responsibilities:

- the Marketing department is ultimately responsible for ensuring that the Organisation uses social media safely, appropriately and in line with the Organisation's objectives;
- the Marketing department is responsible for providing apps and tools to manage the Organisation's social media presence and track any key performance indicators. They are also responsible for proactively monitoring for social media security threats;
- the Marketing department is responsible for working with employees to roll out marketing ideas and campaigns through the Organisation's social media channels;
- the Marketing department is responsible for ensuring requests for assistance and support made via social media are followed up.

Use of Organisational social media accounts

Only people who have been authorised to use the Organisation's social networking accounts may do so.

Authorisation is provided by the Marketing department. It is typically granted when social media-related tasks form a core part of a person's responsibilities.

New social media accounts in the Organisation's name must not be created unless approved by the Marketing department. If there is a case to be made for opening a new account, it should be raised with the Marketing department.

The Organisation's social media accounts may be used for many different purposes.

In general, only post updates, messages or otherwise use these accounts when that use is clearly in line with the Organisation's overall objectives.

Use of personal social media accounts at work

The Organisation recognises that personal social media accounts can generate a number of benefits. For instance:

- making useful industry contacts;
- to discover content to learn and develop in their role;
- by posting about the Organisation, to build awareness of the Organisation online.

As a result, the Organisation is happy for the use of personal social media accounts during working hours provided the use is for Organisational purposes only. All users must ensure it is clear that any personal social media account does not represent the Organisation's view or opinions.

Use of personal social media accounts for personal use is only permitted outside normal working hours e.g. lunchtimes or break times. Use of the Organisation's resources to access personal social media for personal purposes is strictly prohibited however and the user must use their own device.

Usage guidelines

Everyone who operates an Organisational social media account or who uses their personal social media accounts for work based social media reasons must not:

- create or transmit material that might be defamatory or incur liability for the Organisation;
- post messages, status updates or links to material or content that is inappropriate as referred to in the acceptable use section;
- use social media for any illegal or criminal activities;
- send offensive or harassing material to others via social media;
- broadcast unsolicited views on social, political, religious or other non-business related matters;
- send or post messages or material that could damage the Organisation's image or reputation;
- interact with the Organisation's competitors in any way which could be interpreted as being offensive, disrespectful or rude;
- discuss colleagues, competitors, customers or suppliers without their approval;
- post, upload, forward or link to spam, junk email or chain emails and messages.

Regardless of which social networks are being used, or whether a user is using business or personal accounts, following these simple rules helps avoid the most common pitfalls.

- Know the social network. Spend time becoming familiar with the social network before contributing. It is important to read FAQs and understand what is and is not acceptable on a network before posting messages or updates.
- If unsure, don't post. Err on the side of caution when posting to social networks. If an update or message might cause complaints or offence – or be otherwise unsuitable – do not post it. If in any doubt users should consult the Marketing department for advice.
- Be thoughtful and polite. Many social media users have got into trouble simply by failing to observe basic good manners online.
- Adopt the same level of courtesy used when communicating via email.
- Look out for security threats. Be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware.
- Don't make promises without checking. Some social networks are very public. Do not make any commitments or promises on behalf of the Organisation without checking that the Organisation can deliver on the promises. Direct any enquiry to the Marketing department.
- Handle complex queries via other channels. Social networks are not a good place to resolve complicated enquires and customer issues. Once a customer has made contact, handle further communications via the most appropriate channel – usually email or phone.

- Don't escalate things. It's easy to post a quick response to a contentious status update and regret it. Always take the time to think before responding and hold back if you are in any doubt at all.

Private social media use

The Organisation respects a users' right to a private life. However, the Organisation must also ensure confidentiality and its reputation are protected. All employees/affiliates using social media for their private use at any time must ensure:

- it is clear that any personal social media account does not represent the Organisation's view or opinions;
- they conduct themselves in a way that is not detrimental to the Organisation;
- refrain from recording any information about the Organisation that is confidential on any social media platform;
- they take care not to allow their interaction on social media to damage working relationships.

Storing and processing confidential information

In general, confidential information includes anything that is not made available to the public. Information which is highly confidential is information which would cause damage if it were to be revealed to anyone outside of the Organisation. Confidential information also includes any information which is personal to an individual such as their home telephone number (please refer to the Organisation's data protection policy for more information on this).

Users:

- must not share or reveal confidential information including personal information, proprietary data or trade secrets externally (unless prior approval has been given by a member of the Executive Team or a non-disclosure agreement is in place);
- should ask their manager if they are not sure whether information is confidential;
- should not send any documents that are highly confidential by email;
- emails containing information that is in anyway sensitive or confidential should include the following statement:

  The information included in this email is of a confidential nature and is intended only for the addressee. If you are not the intended addressee, any disclosure, copying or distribution by you is prohibited and may be unlawful. Disclosure to any party other than the addressee, whether inadvertent or otherwise is not intended to waive privilege or confidentiality.

Any electronic documents created by users should be stored in a secure location wherever possible. Secure locations are the F drive, P drive or Z drive.

All information held on the F drive is generally open to all users with the exception of certain folders which have restricted access.

Each user has their own personal area on the P drive which only they can access which is where all private/confidential work based documents should be stored. The P drive is a secure location and is backed up to the server.

The Z drive is only to be used for the storage of documents that a user wants to place in the archive. Documents that are saved on the Z drive can be retrieved and reinstated to the F drive if needed.

Locations which are not acceptable for the permanent storage of any Organisational documents include:

- personal computer devices, smartphones and tablets;
- any borrowed equipment (e.g. if presentations are being given on borrowed equipment, the files should be run from an encrypted memory stick or if loaded locally, deleted after;
- C drives on Organisational laptops and desktops.

Where necessary, the above devices may be used as a temporary vehicle for saving documents to the appropriate drive e.g. when taking a photo on a mobile phone to save onto the F drive. When using any device for temporary storage users must always ensure any documentation is deleted from the original source in as timely a manner as possible.

Users must ensure they have a good understanding of how and where things are stored on any devices in their operation so that any deletion of documents is total and permanent. Users should refer to the Organisation's IT contractor for further assistance/training if required.

If any prohibited material is accessed accidentally it must be reported to the IT contractor immediately, otherwise it may be treated as being intentional.

If users are asked by a non-staff member for any details of the computer system, including numbers of computers on site, and software or hardware used, the request should be refused on the grounds that it is against the security policy of the Organisation. Any such requests for information should be referred to the Organisation's IT contractor.

File Encryption

Users **must not** use email to send strictly confidential, sensitive or personal data unless the data files have been encrypted **and** they are only ever sent using Microsoft Outlook (via Office 365) which has end to end encryption built in.

Users that require files to be encrypted must always use 7-Zip software (a free piece of software available to download locally) which offers robust encryption facilities. 7-Zip software allows you to create encrypted copies of your files (referred to as archives) in either *.zip* or *.7z* format. *.7z* format is preferable as many sites block encrypted *.zip* archives. However, if the user is unable to send *.7z* archives in emails *.zip* format can be used instead.

Anyone requiring further assistance with encryption should refer to the Organisation's IT contractor.

Password guidelines

Primary access to the Organisation's network and IT Services is via a network username and password giving access to a set of network services. Any requests for setting up or closing of accounts must be passed to the Organisation's IT contractor (via the HR department). The IT contractor is responsible for the issue and closure of network accounts.

Users are required to follow good security practices in the selection, use and management of their passwords and to keep them confidential in accordance with the prohibited activities on the system and network activities of this policy. Any action taken using a user's account is deemed to have been carried out by that user and for this reason it is vital that passwords are kept secure.

Users are prohibited from the unauthorised use of the passwords of other users unless specific permission has been given for proxy access (e.g. in the case of an unexpected absence).

The following password guidelines are in place and should be followed by all users:

- passwords are to be changed at least every 42 days (passwords will automatically expire every 42 days, users will be prompted in the run up to their password expiry);
- password history will prevent reuse of the last 24 password changes;
- passwords must be:
    - minimum of 7 characters in length
    - not contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - contain characters from three of the following four categories:
      - English uppercase characters (A through Z)
      - English lowercase characters (a through z)
      - base 10 digits (0 through 9)
      - non-alphabetic characters (for example, !, $, #, %)

Leavers

The HR department must be notified as soon as a user leaves so they can contact the Organisation's IT contractor who are responsible for closing the associated accounts.

N.B. Responsibility for retention/deletion of any files held by a user who leaves lies with their head of department and should form part of their department's exit procedure.

Back ups

The Organisation's servers' operating systems are backed up via an iCloud system once every 24 hours which includes:

- F drive;
- P drive;
- Z drive;
- dynamics system;

- thankQ;
- the Intranet server.

Backups hold data for everyday of the most recent month and then prior to that a monthly back up is taken for the previous 7 months.

Periodic checks will be made to ensure back up media can be read and files restored. The Organisation's IT contractor are alerted via an automatic warning if there are any back up issues.

Records of backups will be monitored by the Organisation's IT contractor and be subject to random audit by the Finance Director.

Backup and recovery of individual user files are the responsibility of the user though the IT contractor will make every attempt possible to restore files for users where they have been mistakenly deleted or overwritten.

All requests for documents to be restored from the back up must be approved by a member of the Executive team. Without this permission the Organisation's IT contractor cannot release any documents.

Physical security

Files servers and machines that hold or process highly critical, highly sensitive or high availability data will be located in physically secured areas.

Access to the server room is restricted and controlled by a PIN coded digital lock. Authority to access this area is controlled by the Organisation and administered by the IT contractor and facilities department.

In addition to access control, the server room will also be protected by:

- fire detection systems;
- temperature and humidity control;
- stable, conditioned electrical supply protected by uninterruptable power supply (UPS).

Desktops and laptops owned by the Organisation have password protected screen-savers and automatic log-out mechanisms which operate after 10 minutes of inactivity. However users should always:

- log out of sessions when sessions are finished;
- log out of sessions when leaving their desk (except when only briefly such as going to the printer);
- switch off computers at the end of the working day.

Users should always ensure that portable equipment in their custody is not exposed to opportunistic theft, unauthorised access or observation of sensitive information.

Use of removable media such as USB storage devices on Organisationally owned equipment is forbidden unless there is a genuine business need that can't be fulfilled by an alternative method and prior approval has been given by a member of the executive team.

Where use of any removable media on Organisationally owned equipment has been authorised it must always be virus checked before it is accessed. This includes media from other organisational sites. Instructions for doing this are listed below:

With the USB drive plugged in open My Computer. The USB drive will be displayed in Windows Explorer as a drive letter prefixed with the words removable disk. Right-click on the drive icon, then left click 'scan for viruses' from the drop-down menu. When the scanner starts ensure 'include subdirectory' is ticked and click the green start button. This will scan your USB drive for any viruses and produce a report. Any infected files should either have been deleted or cured. If a virus has been detected users must inform the Organisation's IT contractors immediately.

Users that access the Organisation's network via a personally owned device must always virus check any removable media being used for personal purposes prior to their use. It is important users do this to help safeguard their personal device if the user also intends using it for work purposes.

Licence Compliance

The Organisation strives to be compliant with all licence requirements for software that it uses and maintains systems that easily demonstrate ownership and compliance. Any user that becomes aware of any licensing shortfall must inform the Organisation's IT contractor at the earliest opportunity.

Users may not move or copy software between computers. If software is needed on a machine, users must contact IT contractor.

Software owned by the Organisation must not be installed on a user's personal equipment without prior authorisation but the Organisation's IT contractor.

Audits will be undertaken by the IT contractor on a monthly basis and any unauthorised software will be removed from the system. The list of permissible software is agreed between the Organisation and the IT contractor. The source of unauthorised software will be ascertained and disciplinary action may be taken.

Disposal

All Organisationally owned equipment must be given to the Organisation's IT contractor to ensure secure erasure and destruction of data prior to disposal.

Incident reporting guidelines

Any user who suspects a security incident should report immediately in the first instance to the Organisation's IT contractor and the Organisation's Data Protection Officer who will follow the Organisation's Security Breach investigation plan.

Working on portable devices

The Organisation recognises the inherent dangers of information stored on portable devices (laptops, notebooks, tablets, smartphones etc.) as well as removable media. All users who use portable devices for work purposes (whether the device is owned by themselves or by the Organisation) must adhere to the following guidelines.

Users must not remotely access the Organisation's network and systems except by the means provided by the IT contractor. Access to the Organisation's network is only ever via the 'Garden Organic Gateway' or 'Sonicwall firewall VPN'. Historically the Organisation has also used Microsoft VPN but this is no longer deemed secure enough and should never be used.

Users who use a portable device are personally responsible for its safekeeping and the security of any information it contains.

Rules for the general security of portable devices (applicable to both devices owned by the Organisation and those that are personally owned)

All users must:

- ensure that they use a strong password that adheres to the Organisation's password protocol before using a portable device for work-related purposes (for access security on mobile phones please refer to the specific guidelines on smartphone usage later on);
- Never activate the 'remember me/keep me signed in' setting when entering passwords. Passwords must never be retained or remembered on any portable device. It is the user's responsibility to ensure this is in place across all portable devices in their use.
- never store confidential, sensitive or personal data on a portable device or removable media unless it is encrypted. (please contact the Organisation's IT contractor for further assistance with encrypting if there is a definite and justifiable need to store such information on a portable device). Removable media includes USB drives, external hard drives, CDs or multi-media data storage cards;
- ensure they follow the guidelines for which drives to use when storing all work documents as detailed in the 'storage of confidential information' section - portable devices are only to be used for temporary offline storage and not for long term storage (and never for confidential, sensitive or personal data);
- report the loss or theft of a portable device used for work-related activities immediately to Head Office, the Data Protection Officer and the Organisation's IT contractor;
- always log out of the organisation's server/network between sessions;
- never use open public Wi-Fi networks (i.e. those that aren't password-protected). If there is a genuine and urgent business need users may make use of Wi-Fi if it is a reputable, password protected network. Users should be cautious when assessing whether the Wi-Fi on offer is considered reputable and, if in any doubt, find a more suitable alternative;

- ensure that if family or friends use their devices, they are unable to gain access to any information that is work-related by, for example, password-protecting it;
- ensure that if they delete information, it is deleted permanently rather than left in the device's waste-management system (please refer to the Organisation's IT contractor if further support/training is required in ensuring this happens);
- not install apps, free or paid onto Organisational mobile devices such as smartphones, laptops and tablets unless first authorised by the Organisation's IT contractor;
- be very careful when transporting portable devices - take special care in public, at airport security checks, in cars, in hotel rooms and at conferences and meetings. Consideration must also be given to being watched whilst operating a portable device;

Where an Organisational laptop is no longer required by its original recipient it must be returned to the Organisation's IT contractor so it can be wiped, software reloaded, re-encrypted and redeployed as necessary.

Personally owned portable devices

If a user wishes to use their own portable device for work-related activities, they need to gain written permission from their department head and, once approved, contact the Organisation's IT contractor to be set up to do so.

All users using their own personal laptop/desktop must organise for the Organisation's IT contractor to check their set up is adequate (either physically on site or via a screen connect process) and install the requisite anti-virus/anti-malware software which gives the same level of virus protection as the Organisation's network. Users will not be given permission to work from a portable device without this check and the installation of the software.

All users using their own personal device must still adhere to the '*rules for the general security of portable devices*' as detailed in the previous section.

A user operating a personally owned device must ensure the device is subject to mobile-device management so that if it is stolen, upgraded, recycled or given to family or friends, the user is able to locate the device remotely and delete data on demand.

If a user leaves the Organisation, they must delete all work-related documents and data on their own device prior to their last day with the Organisation.

No personal drives should be connected to any of the Organisation's computer systems or network as this could infect systems with viruses or malware. The use of the following devices is prohibited unless a specific application for use has been made to the Organisation's IT contractor and permission for this use has been granted:

- USB drives/datasticks;
- mobile phones/smartphones/PDAs with local synchronisation;
- external hard drives;
- multi-media data storage cards e.g. SD, MicroSD;

- ipods/MP3 players;
- CDs/DVDs with write capability (read is still permitted);
- any Bluetooth connections;
- digital cameras other than those provided for business purposes.

Smartphones supplied by the Organisation

The Organisation's IT contractor will install and update authorised access and security software on any smartphones issued by the Organisation. However, it is the user's responsibility to prevent unauthorised disclosure of personal or confidential data.

When accessing their work email account users should always access it via the Microsoft Outlook 365 app and never via the web portal as access via the app offers much better security. The Organisation's IT contractor will ensure the app is loaded onto all phones issued by the Organisation.

All Organisational phones will also be set up with either 4 digit PIN number or fingerprint access which must not be removed by the user.

Personal Smartphone usage

It is possible for users to access their work email on their personal smart phone via the Microsoft Outlook 365 app. Users should be aware that by adding their work email to their smartphone the policies that apply to the Organisation's smartphones will then also apply to personal smartphones (as per the previous section). This includes only logging on via the Microsoft Outlook 365 app and setting up PIN number or fingerprint access.

It should also be noted that if a personal smartphone is lost or stolen and it poses a significant risk to the Organisation the user may be asked to remotely wipe their device (of all personal and corporate content). The act of adding a work email to a personal smartphone denotes that a user agrees this is acceptable. It is therefore the user's responsibility to ensure any content on smartphones (both personal and work-based) is backed up at all times.

Use of cloud computing

Cloud computing is defined as access to computing resources, on demand, via a network. Data is transferred to and from the cloud provider, via the network, usually across the internet.

Cloud computing can be deployed using a number of different models:

- private cloud – the cloud customer is the sole user of the cloud service
- community cloud – a group of cloud customers access the resources of the same cloud
- public cloud – available to the general public and is likely to be over the public internet

Processing data in the cloud brings extra risks in terms of information security and compliance with data protection principles. With this in mind the Organisation has an approved list of publicly available cloud computing sites which provide adequate data protection as listed below:

- Dotmailer
- MailChimp
- SurveyMonkey
- Googledrive
- Dropbox

Any user wishing to make use of a publicly available cloud computing site not on the list must first gain permission from the Organisation's IT contractor and Data Protection Officer. Any user wishing to use a new cloud computing site that requires an agreement on terms of service must also have these agreements reviewed and approved by the Organisation's IT contractor and Data Protection Officer.

Particular care must always be taken with the use of publicly available cloud computing and the transferral of personal, sensitive or confidential data. Users must always review whether personal/sensitive/confidential data really needs to be processed via the cloud or whether there may be an alternative method to achieve what is required. If use of the cloud is the only feasible option, any data must be encrypted (please see earlier section on file encryption and, if necessary, refer to the Organisation's IT contractor for further help).

The Organisation also has contracts in place for private cloud operations as listed below, all of whom have been carefully vetted to ensure they are applying correct compliance and governance when processing the Organisation's data.

- Microsoft Office Outlook 365
- Microsoft OneDrive for Business
- Royal London
- Computershare
- ESOS share point
- Citation
- Better Impact
- Lloyds commercial banking
- Bacsactive IP
- Sagepay
- Paypoint
- JustGiving
- Charity's Aid Foundation (CAF)

Any user wishing to appoint a new private cloud provider to carry out a service on the Organisation's behalf involving personal data must first consult with the Data Protection Officer and their head of department to ensure the necessary compliance checks are undertaken prior to any appointment.

Department heads must ensure they have a system in place to record and create, update, suspend and delete user accounts on any cloud computing operations within their department. They must also ensure there are sufficient measures in place to prevent unauthorised access to any data. Extra care must be taken where there are multiple users for a single account e.g. using a cloud

account as a shared area with an external organisation. Department heads must always remove cloud account access from users when they leave the Organisation as part of the department's exit process.

Users must never share cloud computing log-in credentials with co-workers. The Organisation's IT contractor will keep a confidential document containing account information for business continuity purposes.

Cloud service accounts that have been setup for home or personal use must never be used for the storage, manipulation or exchange of company-related communications or company-owned data.

Consequences of non-compliance

If a user is suspected of breaching this policy, the Organisation will investigate the matter. Employees who breach the policy may be subject to disciplinary action up to and including dismissal. Breach of this policy by casual workers, volunteers, associates, Trustees or any other affiliate of the Organisation may result in agreements being terminated.

Users may also incur personal criminal liability for breaching this policy.

External

This policy and the Organisation's privacy notice will be communicated externally by publishing it on the Organisation's website.

Review

This policy will be reviewed and updated before the onset of GDPR in May 2018. Thereafter the policy will be reviewed at 2 yearly intervals to ensure it remains up to date and compliant with the law.

Agreement

This must be signed and returned to the HR department before access is granted to the Organisation's network.

I have read and understood the IT and Information Security policy and agree to adhere to its contents.

Name and position: .....

Signature: .....

Date: .....