POLICY AND PROCEDURE

Information Security Policy

SoLO
Life
Opportunities

38 Walnut Close
Chelmsley Wood
Birmingham
B37 7PU

Charity No. 1102297
England Company No.
5025939

Category: Staff*/volunteers*

Introduction

This document sets out SoLO's Information Security Policies and Procedures, and the responsibilities of everyone using SoLO's systems and IT. Information security is of great importance to SoLO to protect those we hold data on and, in particular, vulnerable people, ensuring compliance with legislation and demonstrating that staff/volunteers within SoLO understand and apply proportionate guidance and process to recording, storing, processing, exchanging and deleting information. Should this not be achieved the organisation can risk the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner.

There are three main principles to this policy:

- All staff/volunteers must consider the sensitivity of the information they handle.
- All staff/volunteers must protect information in proportion to its sensitivity by ensuring that information, whatever its format, is secured by physical means (such as locking paperwork away or appropriately archiving it when no longer current or by using approved electronic means).
- Managers must ensure this policy is applied within their areas of work and should also lead by example.

This policy is mandatory. Any breach of the policy may result in disciplinary action (in accordance with SoLO's disciplinary policy) or, in the case of volunteers, appropriate sanctions being taken.

Any breaches of security (non-compliance with this Policy) must be reported via SoLO's incident reporting process at the earliest opportunity. This is to safeguard SoLO and limit potential damage from information loss.

Policy Statement

It is the policy of SoLO to ensure that all information systems operated are secure and aspire to comply with the requirements of the General Data Protection Regulations and other relevant legislation. It is also the aim of SoLO that all staff/volunteers must be fully aware of the need to maintain secure systems and fully understand their responsibilities as outlined in this document.

All staff/volunteers are responsible for ensuring that they understand and abide by this policy. Failure to do so will be viewed as a serious matter and may result in disciplinary action/sanctions.

Policy Name: Information Security
Organisation: SoLO Life Opportunities
Last Reviewed: new policy
Next Review Date: May 2020
Version 1
Pages in this document - 10

It is the policy of SoLO to ensure:

- Information is protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or negligent action.
- The integrity of information is maintained by protection from unauthorised modification
- Information is available to authorised users when needed.
- Regulatory and legislative requirements are met.
- Contingency plans are produced and tested as far as is practicable to ensure business continuity is maintained.
- Information Security training is provided for all staff/volunteers as part of the Induction Training.
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action taken.
- Sharing of information with other organisations/agencies is permitted providing it is done within the remit of a formally agreed information sharing protocol.
- That there is a fair and consistent approach to the enforcement of standards of conduct expected from employees/volunteers when using social media sites.

Responsibility

All SoLO Staff with access to SoLO's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the equipment and the information that they use or manipulate.

For the avoidance of doubt, the Information Security Policy requires that:

- Individuals must ensure that as far as is possible no unauthorised person has access to any data held by SoLO

- Individuals must ensure that physical security measures are properly used.

- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to SoLO. This includes the proliferation of viruses or other similar computer programmes.

- Individuals will be given access passwords to certain computer systems. These must not be disclosed to other members of staff. They should not be written down in any identifiable manner and they should be changed regularly.

- Individuals must not load or download software packages onto SoLO's PCs and under no circumstances should games software be loaded onto SoLO's PC's unless they are used, legitimately for the delivery of projects for members.

- Any staff found to be storing large numbers of personal files, especially large files such as photographs or videos may be asked to remove them or in some circumstances be the subject of disciplinary action.

- Any files received on any media, brought or sent into SoLO or files received by electronic mail must be virus checked before being loaded onto a SoLO device. SoLO provides a virus checker for this purpose, but where there is doubt about the source of a file, advice must be sought from the ICT provider before downloading.

- All staff/volunteers must read, understand and sign to acknowledge that they have read and accepted this policy and the specific requirements of it, which are as follows:

Network Security

- Only SoLO owned Tablets, Laptops and PC's are allowed to be connected to the main server.
- If remote access is required, permission must be gained from a Senior Manager

Physical Security

- Access to data held on SoLO's information systems is minimised by restricting physical access to SoLO's buildings.
- Where information is kept in the SoLO offices, access to buildings is restricted by ensuring that security doors are closed properly and that entry codes are kept secure and changed regularly.
- Doors and windows must be secured at lunch times and overnight and at all times when the office is left unattended.
- PC's will be set up to log off automatically after short periods of inactivity.
- Visitors to SoLO's buildings must be accompanied at all times and signed in and out of the premises on arrival and departure.

Computer Security

1. Data Storage

All staff must abide by the rules of the GDPR.

- Access to server is controlled by passwords and only to be accessed by authorised personnel.
- Storage of data on PC or Laptop's C: drive is discouraged and all users are requested not to store files on PC or Laptop's C:\drives because in the event of failure, all data stored on the C: drive would be lost as it not backed up.
- All information related to SoLO business is to be stored on the S Drive. This is a secure storage area which is regularly backed up and is therefore resilient to failure.
- Photos and videos can only be stored if they relate explicitly to business needs.

2. File Storage and Naming Conventions

- All documents and files should be given clear and descriptive titles that will help others to understand what is contained within them.

- Information which is no longer required should be promptly disposed of by deletion or destruction. Wherever possible, older versions of documents should be immediately archived.

- To avoid error, documents should only be stored in one area.

3. Screen Locking

- Computers must not be left unattended with screen unlocked when logged in to SoLO's Network.

- Whenever staff move away from a workstation they must ensure that they have logged off or locked the workstation.

- When leaving a place of work staff must ensure they have logged off and closed down the workstation correctly.

4. Memory Sticks and removable media

- Only SoLO supplied encrypted memory sticks or external hard drives are to be used.

- Confidential data must not be stored on memory sticks.

5. Passwords

- Passwords given to staff are for individual use only.

- Passwords should not be written down in a recognisable format or given to others to use under **any** circumstances.

- Passwords must not be easily recognisable – avoid family names.

- Passwords must be changed every 6 months as a minimum.

- If a Line manager needs access to a staff members computer, for example if they are off sick, or on annual leave, the Line manager must contact the Business Support Manager for permission.

6. Viruses

- All files received on disc from outside SoLO or received via electronic mail must be checked for viruses before being used on SoLO equipment. Staff must not intentionally introduce/send or download files or attachments which contain viruses, or which are meant to compromise the SoLO systems.

- If a virus is suspected, the ICT provider must be informed immediately. The workstation should not be used until given permission from the ICT provider and a sign stating this should be placed on the workstation to warn other users. Any disks, CD ROMS, and USB memory sticks that have been used on the suspected infected workstation should be gathered together and not used.

7. 3rd Party Network Connections

- All requests for external 3rd Party network connections must be processed by SoLO's ICT Provider and will be strictly governed by relevant standards and approval process.
- When there is a necessity for remote support from the ICT provider, all other windows must be closed down so that confidential data is not shared with the operative.

Document Handling

All paper documents should be securely locked away when no longer required, by being placed in appropriate secure containers.

The clear desk policy requires that all confidential information shall be put away and locked when the desk is unattended.

Printing

Staff/volunteers must ensure adequate care is taken when printing information that is confidential and ensure that it is not left in view.

Scanning

Staff must ensure adequate care is taken when scanning confidential documents and remove from the scan file immediately by either re-siting into an appropriate folder or deleting. The Admin Staff will regularly review the folder and promote removal where this has not happened.

Clear Desk

All confidential data must be locked away at the end of each day.

Mobile Workers and Home Workers

1. Laptops

- Care must be taken to avoid being overlooked whilst using SoLO equipment in any public area
- Laptops must be kept in a secure location when not in use.
- Laptops must not be left unattended during the normal working day unless it is on SoLO premises where there is good physical security at entrances to the building.
- When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it.

2. Home Computers

- If staff are using home computers for any SoLO related work, they must ensure that they are password protected, in a secure location, not in public view and any files saved should be kept on a SoLO encrypted memory stick.

3. Manual Files

- Manual files processed outside of SoLO's property must be kept with the individual completing this work.
- When left unattended, Manual Files must be, where possible, in a locked container and out of view.
- Computer equipment or manual files that are travelling with an employee must be locked in the boot of the car or kept with the individual at all times when travelling by public transport.
- Computer equipment or manual files must not be left unattended on public transport or left in a vehicle overnight.

4. Home Printing

- Home printing is only permitted in exceptional circumstances where a business case has been approved by the Line Manager

Mobile Devices

- Staff issued with mobile devices are responsible for safekeeping and security.
- Security lock and pin protection must be used where available to protect the device and any stored data.
- Passwords must not be shared.

1. Lost or stolen mobile devices

- If a mobile device is lost or stolen, staff must;

  1) Contact the office or on-call immediately.
  2) Complete an incident report
  3) Notify the local Police station of the loss.

Please note that replacement of lost or stolen handsets is not covered by any insurance so the cost will come out of the project's equipment budget.

2. Leaving SoLO or moving into another role

- Staff who are issued with any mobile devices must ensure their safe return on termination of employment or acceptance of a different post within SoLO which does not require the use of a those devices.

Use of the Internet

1. Downloading of Information Resources

- Individuals must not download non-work related information from the Internet. To reduce the likelihood of a virus infection.
- Individuals must take care to ensure that the files are from a trustworthy source. Individuals requiring any new software, including any plug-ins, must make a formal request to the ICT Provider, after clearing with their Line Manager.
- Software must not be downloaded and/or installed onto SoLO ICT equipment unless it has been approved by the Line Manager and can be validated that it is licensed for current use.
- Graphical, audio and video files may be downloaded and stored on SoLO's network for business use only.
- Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any SoLO work.

2. Uploading data/Information to the internet.

- Any users who are responsible for uploading data/information to the internet must be sure that the information being uploaded is suitable to upload, and not **confidential.**

3. Internet Filtering and Blocking

- Users should not attempt to by-pass the SoLO's Internet filtering software.

- Staff who encounter a commonly used business site which is blocked and have genuine business reasons for accessing that site frequently may contact the ICT provider for permissions, after approval from their Line Manager.

Use of Email

E-Mail is a useful tool that enables individuals to organise themselves and communicate with others. This policy sets out the expectations for all SoLO computer equipment users who are provided with access to Outlook. Outlook is provided as a business tool and should not be used for non-work related matters.

1. Sending email

- E-mail is set up by default to conform with SoLO branding and agreed signatures.All staff must use this default setting, that includes name, title, service and contact details.

- All e-mails must have the subject line completed and should be checked for accuracy of spelling, punctuation and grammar. Bold text should only be used sparingly, and for emphasis, and underlining should only be used for links. The use of upper case text should be avoided as this may be interpreted by recipients as shouting.

- To avoid information overload, individuals should consider carefully who needs to be included in any e-mail and whether face-to-face or telephone contact could be an alternative method. When sending confidential data, individuals should, wherever possible, password protect the document and send password by a different method (e.g. text)

- Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.

- Individuals must not use other people's mail accounts nor attempt to impersonate someone else or appear anonymous when sending e-mail.

- Individuals must only forward emails where the information in the trail is appropriate for the recipient to see.

2. Distribution lists

- Send to all should be avoided and staff should be mindful about who they copy emails into.

3. Mailbox management

- Staff are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate.

- Staff should only archive and retain messages that need to be kept and these should be selected in line with business need. All other e-mail that does not constitute a necessary record of business should be deleted once it is no longer required.

- When an email is received with an attachment which needs to be retained, individuals should save the attachment to the shared drive, and not leave the attachment within the email.

4. Misuse of email

- Staff must not send or forward any abusive, threatening, defamatory or obscene messages. Likewise staff should avoid sending messages in the heat of the moment, taking time to reflect on drafts and how they may be interpreted before sending them.

- Staff must take care with any suspected malicious or nuisance e-mails received (e.g. chain e-mail, hoax and spam e-mails) and delete them. If any suspicious e-mails are received they should be reported to the ICT service provider.

- Staff must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

5. Mail and absence

- An "Out of Office" notice must be used whenever a staff member is away from their normal office base, and messages should clearly indicate a date of return and contact details for those who can deal with issues whilst the individual is away.

- To avoid the necessity of others accessing an individual's computer, the staff member must make provision to re-direct their emails to another appropriate individual within their team whilst they are away from work for more than 3 working days.

6. Calendars

- Calendars should be set to be viewable by SoLO office staff. Consequently, it is important that individuals use the "private" option for all confidential appointments.

- Staff are required to keep their calendars up to date, and should indicate their whereabouts when away from their normal office base.

7. Attachments

- Attachments should not be included in any internal mails or meeting invites, wherever it is possible links to documents on the server should be used instead/

Security Incident Reporting

- Information Security Incidents must be reported within 24 hours in accordance with SoLO's Incident Policy

- Loss of **any** piece of ICT equipment is classed as a security incident and must be reported.

Manager's Responsibilities

- All Managers and Project Leaders must abide by all the guidelines and procedures as set out and agreed in this document.

- Managers must follow the New Starter process to ensure that new staff who require access to ICT are provided with log-in credentials and access privileges as appropriate.

- Managers must also take responsibility to ensure that new staff are aware of this policy.

- Managers must ensure that the users work related information, e-mails and data is transferred, if required, to the respective working directory for future access on the system or is deleted. This will ensure that the appropriate security is maintained on leavers information and data.

Leavers - return of IT equipment and documentation

- When an employee leaves SoLO, Line Managers must ensure all IT equipment and physical files are returned to SoLO, and delete their accounts.

- On the last working day, Managers must collect all the leavers IT equipment and ensure it is returned to the office.

- Failure to comply with the requirements of this policy in relation to the return of ICT equipment is regarded as a serious breach of this policy.

Controls

It is up to all managers of staff in SoLO to ensure that individuals adhere to this Policy. Managers will be responsible for monitoring systems under their control for signs of:

- Illegal or unauthorised software having been loaded.
- Password misuse.
- Unauthorised access

Spot checks will also be made to ensure that where data is not held and backed up centrally, adequate backups are being made.

Acknowledgement and Acceptance

Each user must read, understand and sign to verify they have read and accepted this policy.
I understand and agree to comply with the Information Security and Acceptable Use of IT Policy of my organisation.

(Volunteers will be required to sign the acceptance as part of their volunteer agreement)

Signature of User: ……

Name of User (please print)……

Job Title: …… Date:……

Linked to Policies:

- **GDPR**
- **Office Security**
- **Incident Reporting**
- **Confidentiality**
- **Social media**