

Security Policy

Compass Disability Services

Units 11 – 12 Belvedere Trading Estate
Taunton, TA1 1BH

September 2016
Review date: September 2021

Introduction

Compass Disability Services places great importance on ensuring the security and safety of our employees, our assets, and the information that we process, store and the methods used to destroy it. We strive to take all necessary steps to protect our employees, assets and information as far as possible and ensure they remain secure.

Scope

This policy applies to:

- People – meaning customers and all staff and volunteers working for Compass Disability Services and its projects.
- Assets – meaning the buildings and their contents, including equipment provided for homeworkers such as laptops, mobile phones for example.
- Information – meaning all paper and electronic records relating to identifiable individuals.

This policy broadly sets out Compass Disability Services' position regarding security measures; however more details regarding specific aspects of information security are contained within the Data Protection Policy, security of lone workers is covered in more detail in the Lone Workers Policy and some security measures are also dealt with in the Confidentiality Policy. The term security should not be confused with confidentiality; however there must be a relationship between the two.

Security of Assets

Compass Disability Services operates a number of security measures which aim to safeguard the organisations assets as far as possible.

Intruder Alarm

Compass Disability Services' premises with the exception of Shopmobility, are fitted with an intruder alarm which must be activated whenever the premises are not in use. Prior to leaving the building the member of staff responsible for the 'close down' must follow a checklist of duties to complete, such as ensuring all windows are closed and doors are locked. Members of staff that are responsible for the 'close down' will be made aware of the necessary procedure and shadowed until they are comfortable performing this task, at which point it will be signed off in their training folder. The checklist is available on the server and staff are encouraged to

Date updated: 23/05/2017	By whom: Tony Biggs	Version number: 4
Location: Z:\Compass Files\Strategic & Governance - Gov\Policies\Policies in Force - Version Controlled\Security Policy\Security Policy.doc		

follow the checklist. Failure to follow the prescribed checklist or set the intruder alarm may result in disciplinary action being taken.

The intruder alarm code is restricted to employees who have been issued with office keys or who need to activate or deactivate the alarm in the course of their duties, i.e. Facilities Support Workers who require access to the Mendip room. Building keys are only issued to employees that are regularly required to unlock or lock the offices; all building keys must be signed for when they are issued to ensure an accurate log of key holders is kept.

It is preferable that external parties carry-out any work during opening hours when members of staff are present; however there may be rare occasions when a known and approved contractor will require access to the building to make repairs, carry out tests, install new equipment, etc. The Site Manager is responsible for ensuring that the contractor is able to enter the building and reset the alarm behind them. The Site Manager is further responsible for ensuring that the intruder alarm code is changed as soon as possible after works have been completed and reissued to relevant staff.

In the interests of maintaining a high level of security the intruder alarm code will also be changed whenever a key-holding member of staff leaves the employment of Compass Disability Services. It is the responsibility of the Site Manager to ensure this occurs and all code holding members of staff are informed.

Visitors and Access to Office / Back Areas

Access to office/back areas is restricted to members of staff, Trustees and appropriate volunteers. Visitors should report to reception on arrival and will only be able to access office/back areas when accompanied by a member of staff or with the permission of a senior team member. Leaving a visitor unattended may be unavoidable if, for example, the staff member has to leave a room to collect paperwork or visit the toilet, however consideration should be given to how trustworthy a visitor is before allowing them to stay unattended in office/back areas. If the visitor is unknown or considered high risk then they must be asked to return to reception until they can be accompanied further. Where possible it is critical that equipment is stored in the appropriate place with cupboard doors and curtains closed to conceal any articles of value as much as possible in order to avoid any unnecessary temptation to unaccompanied visitors.

Home Workers Assets

Computers, laptops and mobile phones are used by home working employees and they are made aware of the need to apply security practices to the use of this equipment at home, to the same extent as if it were in the office, for example ensuring that data is stored securely and equipment is password protected.

Due to the increased risk of theft and potential security issues staff are advised not to take any excess equipment or information with them outside of the office or leave equipment/information unattended, in their car for example. However, it is recognised that practically this may be necessary on occasions, therefore staff

Date updated: 23/05/2017	By whom: Tony Biggs	Version number: 4
Location: Z:\Compass Files\Strategic & Governance - Gov\Policies\Policies in Force - Version Controlled\Security Policy\Security Policy.doc		

must make sure that information is out of site and locked away, e.g. in the boot of their car.

Disposal of Assets

Whenever a piece of equipment that has contained personal or confidential information (such as computer hard drive or mobile phone) reaches the end of its useful life, Compass Disability Services will ensure that any such information is permanently removed and destroyed, for example a mobile phone SIM card will be shredded; our IT service provider will ensure that any information relating to Compass Disability Services or its associated projects, is permanently wiped from the hard drive and it will then be disposed of in an appropriate manner.

Personal Property

Compass Disability Services cannot accept liability for any damage to, loss, or theft of personal property including vehicles, and employees are strongly advised not to bring valuables in to the work place and where this is unavoidable not to leave them unattended at any time.

In order to protect the organisation's property and employee's alike, if it is believed that a crime such a theft or criminal damage has been committed, the police will be called to deal with the matter. All staff, Trustees and volunteers are duty bound to fully cooperate with any police investigation.

Information Security

The security of personal information is very important to ensure data remains safe and Compass Disability Services is compliant with the Data Protection Act 1998. Our Data Protection Policy addresses security issues relating to personal data and should be consulted for further information.

Compass Disability Services encourages a culture of openness, honesty and accountability in which positive challenge to inappropriate behaviour is part of normal practice. Consequently, all staff are encouraged to air any concerns they have, this stance is supported by our Whistle Blowing Policy and Procedures that are in place to protect any employee who suspects wrongdoing, such as an internal security breach.

Safe

Compass Disability Services has 3 fire and waterproof safes that are not easily moveable, located in the Finance office, Payroll office and Compass Wellbeing office. The purpose of the safe is to ensure maximum security can be provided to smaller items of high importance. The access code to the safe is restricted to a small number of employees, ensuring that there is always someone onsite during office hours with access to the safe.

In the interests of maintaining a high level of security the safe code will also be changed whenever a key-holding member of staff leaves the employment of

Date updated: 23/05/2017	By whom: Tony Biggs	Version number: 4
Location: Z:\Compass Files\Strategic & Governance - Gov\Policies\Policies in Force - Version Controlled\Security Policy\Security Policy.doc		

Compass Disability Services. It is the responsibility of the Site Manager to ensure this occurs and all key holding members of staff are informed.

Cash Handling

Compass Disability Services accepts that cash is particularly vulnerable and will have cash handling procedures in place to ensure that cash is handled appropriately and that floats and takings are monitored and banked regularly. Staff will undergo training to ensure that cash is handled effectively and in line with procedure, failure to do so could lead to disciplinary action being taken.

Training

Security issues are of relevance to all members of staff and volunteers at Compass Disability Services; therefore it is imperative that all staff are aware of their responsibilities. All staff and volunteers are given time to make themselves familiar with this policy (and other related policies E.g. Data Protection, Confidentiality) and will have their security responsibilities specific to their role within the organisation outlined upon induction.

Responsibilities

The Board of Trustees recognises its overall responsibility for ensuring that Compass Disability Services complies with its legal obligations, which is managed by the Chief Executive Officer. Day to day aspects of physical and technical security is undertaken by the Site Manager on behalf of the CEO.

Some members of staff have specific responsibilities with regards to the security aspects of the organisation, which will be outlined in their job description. In addition all members of staff have a responsibility to be alert to any external security threats and report any unusual activity, suspected security breaches, etc to either the Site Manager or the CEO as a matter of urgency.

Policy Revisions

This policy will be reviewed and amended every five years or as necessary to ensure compliance with any changes or amendments to any relevant legislation or changes to the operations or premises of Compass Disability Services.

All staff or volunteers should pass suggestions or recommendations for the revision of any aspect of the policy through normal channels to the Chief Executive Officer.

Additional Information:

- Data Protection Policy
- Lone Worker Policy and Procedures
- Confidentiality Policy
- Whistle Blowing Policy and Procedure

Associated documents and files:

Building Closedown Procedure
Building Closedown Checklist
Building Opening Procedure

Date updated: 23/05/2017	By whom: Tony Biggs	Version number: 4
Location: Z:\Compass Files\Strategic & Governance - Gov\Policies\Policies in Force - Version Controlled\Security Policy\Security Policy.doc		

Building Opening Checklist

Date updated: 23/05/2017	By whom: Tony Biggs	Version number: 4
Location: Z:\Compass Files\Strategic & Governance - Gov\Policies\Policies in Force - Version Controlled\Security Policy\Security Policy.doc		