DISABILITY POSITIVE INFORMATION SECURITY POLICY

Revision History

Version	Revision Date	Revised by	Section Revised
1.7	22/11/2018	JF	No changes Made
1.8	12/11/2019	LT	1, 5, 6.4, 6.5.1
1.9	23/11/2020	LT/MC	6.5, 6.6, 6.6.1, 6.6.2, 8
	30/11/2021	Annual Review – no changes	
	30/11/2022	Annual Review – no changes	

Document Control

Document Owner: **LT**	**Document No:** **8.1**	**Approved by:** **Approved**	**Date Approved:** **23/11/2020**
Security Classification: High	**Next Review Date:** **30/11/2023**	**Version:** V1.9	**Department:** **Operations**

1 INTRODUCTION

Disability Positive *(hereinafter referred to as the **"Company"**)* has an extensive and robust Information Security Program that consists of a vast array of policies, procedures, controls and measures. This Information Security Policy is the foundation of this program and ties together all other policies as they relate to information security and data protection.

The Company Information Security Policy covers all aspects of how we identify, secure, manage, use and dispose of information and physical assets as well as data security expectations, remote access, password and encryptions. To ensure that the importance of each information security area is not missed or vague, we use separate policies and procedures for each information security area and where applicable, reference these external policies in this document.

All information security policies and procedures should be read and referred to in conjunction with each other, as their meaning, controls and measures often overlap. The policies and documents that form part of the Company ***Information Security Program are: -***

- Information Security Policy
- Confidentiality Agreement
- Remote Access Policy
- Access Control Policy
- Data Retention & Erasure Policy
- Data Protection Policy & Procedure
- Asset Management Policy
- Supplier Policy
- Risk Management Policy & Procedures
- Business Continuity Plan

2 POLICY STATEMENT

Information and physical security is the protection of the information and data that the Company creates, handles and processes in terms of its confidentiality, integrity and availability from an ever-growing number and wider variety of threats, internally and externally. Information security is extremely important as an enabling mechanism for information sharing between other parties.

The Company are committed to preserving Information Security of all physical, electronic and intangible information assets across the business, including, but not limited to all operations and activities.

We aim to provide information and physical security to: -

- Protect client and 3rd party data
- Preserve the integrity of The Company and our reputation
- Comply with legal, statutory, regulatory and contractual compliance
- Ensure business continuity and minimum disruption
- Minimise and mitigate against business risk

3 PURPOSE

The purpose of this document is to provide the Company's statement of intent on how it provides information security and to reassure all parties involved with the Company that their information is protected and secure from risk at all times.

The information the Company manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

4 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5 OBJECTIVES

The Company have adopted the below set of principles and objectives to outline and underpin this policy and any associated information security procedures: -

- Information will be protected in line with all our data protection and security policies and the associated regulations and legislation, notably those relating to data protection, human rights and the Freedom of Information Act
- All information assets will be documented on an Information Asset Register (IAR) by Head of Finance and will be assigned a nominated owner who will be responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it
- All information will be classified according to an appropriate level of security and will only be made available solely to those who have a legitimate need for access and who are authorised to do so
- It is the responsibility of all individuals who have been granted access to any personal or confidential information, to handle it appropriately in accordance with its classification, the data protection principles and signed confidentiality agreement

- Information will be protected against unauthorised access and we will use encryption methods as set out in the above objectives in this policy
- Compliance with this Information Security and associated policies will be enforced and failure to follow either this policy or its associated procedures will result in disciplinary action

The Chief Executive Officer has the overall responsibility for the governance and maintenance of this document and its associated procedures and will review this policy at least annually to ensure this it is still fit for purpose and compliant with all legal, statutory and regulatory requirements and rules. It is the responsibility of the Management Team to ensure that these reviews take place and to ensure that the policy set is and remains internally consistent.

6 PROCEDURES & GUIDELINES

6.1 SECURITY CLASSIFICATION

Each information asset will be assigned a security classification by the asset owner, which will reflect the sensitivity of the asset. Classifications will be listed on the Information Asset Register.

6.2 ACCESS TO INFORMATION

Staff at The Company will only be granted access to the information that they need to fulfil their role within the organisation. Staff who have been granted access must not pass on information to others unless they have also been granted access through appropriate authorisation. ***Refer to the Company's Access Control Policy for protocols and more information.***

6.3 SECURE DISPOSAL OF INFORMATION

Care needs to be taken to ensure that information assets are disposed of safety and securely and confidential paper waste must be disposed of in accordance with relevant procedures on secure waste disposal. Where an external shredding service provider is employed, secure paper disposal bins are in the office and used in all instances of confidential paper disposal.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Company, unless the disposal is undertaken under contract by an approved disposal contractor.

In cases where a storage system *(for example a computer disc)* is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. ***Refer to the Company's Retention Policy for protocols and more information.***

6.4 Information on Desks, Screens and Printers

Having a clear desk expectation enables the Company to maintain efficiency and an effective workplace and secures the personal information that we must hold owing to the nature of our business. As a Company, we have a full understanding of the requirements to protect personal information and we believe that having a **clear desk environment** is pivotal to this end.

The Company expect staff to maintain clear desks at all times. Members of staff who handle confidential paper documents should take the appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

At the end of the working day, all employees are expected to tidy their desk and to tidy away all office papers into locked desk drawers and filing cabinets. The Office Manager will also do an office walk round to ensure that paper data has been locked away or destroyed before leaving the office.

It is not just personal information relating to customer or employees that are bound by the clear desk approach. All paper formats, including those used to write information down can be considered private or personal information and are subject to the same policy governance rules. Such documents can include, but are not limited to: -

- Telephone notes
- Printed emails
- Notices and minutes of meetings
- Disciplinary letters
- References
- Accounting paperwork
- Draft letters
- Report and Management Information
- Corrective Action Plans
- Registers and Visitor Sign-in Books
- Manuals

6.5 Data Security

The Company prefers communication to be sent by electronic means rather than by post, wherever possible. All staff are expected to check that the information they are sending is for the intended recipient. Such checks should include, but is not limited to: -

- Sensitive and personal communication/documentation/payslips etc must be sent out via secure email (e.g. egress – confidential or .NET equivalent for PHB information where appropriate)
- All recipients email addresses must be double-checked before sending an email. To ensure that the potential recipient is who the employee is intending to contact,
- Particular care should be taken where the email address for the client does not contain their name (e.g. if the client is called John Smith, but the email address doesn't have John or Jsmith in the name), please make sure it is correct and belongs to the intended recipient.
- Every email attachment must be opened once attached to an email, to ensure it is correct and only contains information for the intended recipient/relevant attachment.
- Verify what client authorisation is held on file, in terms of who is authorised to receive information/communications, before providing any information.
- Where staff are emailing a group of people, this must be sent as a blind copy (BCC) email to the recipients. The field completed should be double-checked before sending an email.
- Any email forwarded, if it includes details of the original sender and they have not given permission to share it must not be forwarded outside the Company without their permission.
- Where it is not possible to send information via email, any post must be double checked, to ensure it is correct and only contains information for the intended recipient, before the envelope is sealed and posted. Content must be checked that the person you intend to post the information to, is the same person you are actually posting it to and does not have any other recipient's information inadvertently included.
- Check the sender's email address before responding or clicking on any links. Refer to 6.5.1 for further information.

6.5.1 Beware of Phishing emails

Make sure that any emails received are legitimate and not phishing emails designed to harvest credit card details and personal data. Treat such emails with suspicion and examine the senders address and the content very carefully (Phishing emails can look identical to an internal email, but often the language used may not seem quite as expected, or the font may be different or there will be no Company or Charity number on the bottom of the email). Fraudsters are quick to latch onto people' s generosity to see if they can tempt you, or the Company, to part with cash. Report any suspicious looking emails immediately to Management.

Some emails contain an attachment or malicious link which, when opened, will trigger software to scramble all data. This ransomware is designed to encrypt all the files on a computer, and even on servers. The best defence is to not succumb to 'clickbait'. If the sender email doesn't look valid, do not click on links and do not double click on every email

attachment. Pick up the phone to check that any email is legitimate, before clicking any links or downloading attachments. Report any suspicious looking emails immediately to Management.

6.6 DATA ENCRYPTION

Definitions

Encryption: This is the process of locking up (*encrypting*) information using cryptography. Such information appears illegible if accessed, unless a corresponding key is used to decrypt the data.

Decryption: The process of unlocking the encrypted information via a key.

Encryption methods are always used to protect confidential and personal information within The Company and when transmitted across data networks. We also use encryption methods when accessing The Company network services, which requires authentication of valid credentials *(usernames and passwords)*.

Where there is a requirement to remove or transfer personal information outside of The Company, it is always kept in an encrypted format. Encryption is used whenever appropriate on all remote access connections to the organisation's network and resources.

All confidential and restricted information transmitted via email is encrypted ie. Egress.

6.6.1 ENCRYPTION ALGORITHMS AND PROTOCOLS

The Company use a variety of encryption methods dependant on the nature of the information being stored or transferred, its location and its use.

6.6.2 REMOTE ACCESS

It is the responsibility of all the Company employees with remote access privileges to the company network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to The Company. ***Refer to our Remote Access Policy for protocols and more information.***

- Secure remote access must be strictly controlled
- At no time, should any the Company employee provide their login or email password to anyone else
- The Company employees with remote access privileges must ensure that their Company owned computer, which is remotely connected the company network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
- All hosts that are connected to The Company internal networks via remote access must use the most up-to-date anti-virus software as provided by the company on supplied computers

6.7 Firewalls & Malware

The Company understands that adequate and effective firewalls, malware and protected gateways are one of the main and first lines of defence against breaches via the internet and our networks.

We utilise configured firewalls and have daily anti-virus applications running on all computers, networks and servers. The IT outsourced management service is responsible for checking the log of all scans and for keeping these applications updated and compliant.

Systems are regularly scanned and assessed for unused and outdated software with the aim of reducing potential vulnerabilities and we routinely remove such software and services from our devices where applicable.

The IT outsourced management service also has full responsibility for ensuring that the latest application and software updates and/or patches are downloaded and installed, keeping our security tools current and effective. Security software is reviewed and updated monthly, or sooner where updates or patches have been released.

7 Security Breach Management

7.1 Introduction

The Company's definition of a breach for the purposes of this and related documents, is a divergence from any standard operating procedure (SOP), which causes a failure to meet the required compliance standards as laid out by our own compliance program objectives and/or those of any regulatory body.

Compliance in this document means any area of business that is subject to rules, laws or guidelines set out by a third party which are to be followed and which, when breached, could cause emotional, reputational or financial damage to a third party.

7.2 Breach Management Approach

The Company has robust objectives and controls in place for preventing security breaches and for managing them if they do occur. Due to the nature of our business, the Company processed and stores a vast amount of personal information and confidential client data and as such, require a structured and documented breach incident program to mitigate the impact of any breaches. Whilst we take every care with our systems, security and information, risks still exist when using technology and being reliant on human intervention, necessitating defined measures and protocols for handling any breaches.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating

actions are in place where necessary, however should there be any compliance breaches, we are fully prepared to identify, investigate manage and mitigate with immediate effect and to reduce risks and impact.

The Company have the below objectives with regards to Breach Management: -

- To maintain a robust set of compliance procedures which aim to mitigate against any risk and provide a compliant environment for trading and business activities
- To develop and implement strict compliance breach and risk assessment procedures that all staff are aware of and can follow
- To ensure that any compliance breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Compliance Breach Incident Form for all breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To comply with regulating bodies and laws on compliance breach methods, procedures and controls
- To protect clients and staff – including their data, information and identity

Please refer to our Data Breach Policy & Procedures for further details.

8 RESPONSIBILITIES

All information users within the Company are responsible for protecting and ensuring the security of the information to which they have access. Managers and staff are responsible for ensuring that all information in their direct work area is managed in conformance with this policy and any subsequent procedures or documents. Staff who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

The Company will ensure that staff do not attempt to gain access to information that is not necessary to hold, know or process and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.