DISABILITY POSITIVE REMOTE ACCESS POLICY

Revision History

Version	Revision Date	Revised by	Section Revised
1.3	18/11/2018	JF	No Changes
1.4	12/11/2019	LT	5 onwards – Personnel changes and VPN/Microsoft Remote Desktop Connection
1.5	23/11/2020	LT/MC	All – removal of Bring your own device.
	30/11/2021	Annual Review – no changes	
	30/11/2022	Annual Review – no changes	

Document Control

Document Owner: **LT**	**Document No:** **8.4**	**Approved by:** **Approved**	**Date Approved:** **23/11/2020**
Security Classification: Low	**Next Review Date:** **30/11/2023**	**Version:** V1.5	**Department:** Operations

Copyright © 2022 | Disability Positive

1 INTRODUCTION

Disability Positive *(hereinafter referred to as the **"Company"**)* operates a controlled approach to remote access (*or teleworking*) and understands that due to the nature of our business, working from outside of the office is a necessity. However, we also appreciate the additional risk posed by remote access and working off-site, as such, have documented procedures and rules that must be followed.

For the purposes of this policy, ***'remote access'*** refers to any work that takes place off-site and requires the use of any Company equipment (information assets). This includes working from home, using Company laptops, access to the Company network or taking Company information off-site.

Where client visits and travel are often a necessity, being able to access the Company information systems are an important part of our service, however we have strict protocols for security and restriction that apply to all employees and managers.

Remote access utilise devices provided by the Company for outreach working or working from home. This enables the Company to secure, register and monitor such devices.

2 POLICY STATEMENT

It is the Company's policy to permit remote access where there is a genuine business need, but only with prior permission and in accordance with the rules of this policy. Security measures must be enforced, and all employee agree to the terms of this document when working off-site.

The Company remains the data controller and recognises its legal obligation to abide by the data protection laws. We place a high value on the information assets within our remit and aim to protect them at all times. All users are expected to adhere to the standards in this policy and agree to keeping data and devices secure, updated and safe.

3 PURPOSE

The purpose of this policy is to outline the Company's approach, objectives and guidelines for remote access activities. It documents methods of access and reasons for using remote access and places restrictions on these functions to ensure effective security for the Company, its clients and our employees, as well as protecting the personal data that we hold.

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.

Copyright © 2022 | Disability Positive

The Company authorises remote access on a case by case basis and reserves the right to refuse, prevent or withdraw access to users at any time.

5 OBJECTIVES

The Company permits the use of remote access to better serve our clients and customers and to offer more flexibility to employees when they need to access the Company systems off-site.

However, due to these devices and practices needing additional security, the Company have developed and abide by this policy to provide guidance and requirements of remote access.

With regards to remote access, the Company ensures that: -

- Has a robust and maintained Remote Access Policy that is compliant and disseminated
- All users are made aware of this policy and understand their responsibility and commitment to its rules by signing a Company Equipment Responsibility Form
- All employees are provided with a Company owned laptop, that must be used for remote access.
- Company owned equipment should only be used for Company business and never be used for personal use.
- The Company reserves the right to ensure that Company equipment are using up-to-date and effective firewalls, malware and anti-virus software
- We utilise strong encryption and secure access connections for all remote access
- Where a user from a remote access location or connection uses unrecognised credentials 3 times, their device and access will be blocked until authentication by the IT Support Service.
- All remote access connections are secured with passwords and must follow the Company's strong password protocols as detailed in the Access Control Policy
- The IT Manager can restrict access instantly and erase connections and data on Company equipment.
- No personal equipment or client equipment can be used for remote access.

5.1 REMOTE ACCESS PROTOCOLS

Employees are required to access the Company assets and/or networks whilst off-site. Such remote access is heavily governed and controlled to prevent additional security risks and to protect the device being used, the Company network and infrastructure and the information being accessed.

All users via remote access are required to: -

Copyright © 2022 | Disability Positive

- Take appropriate security measures to protect the device and the information being accessed
- Complete and sign a Company equipment form
- Protect their device from being seen, used or copied by unauthorised individuals
- Access the network via the authenticated network using secure connections

The Management Team has overall responsibility for any device used off-site and connecting to the Company network via remote access.

The Management Team must: -

- Ensure the device used for remote access has where applicable a firewall, anti-virus software and secure password login
- Register each remote access device and log who uses it and on what device
- Maintain control and access connection to the Company's network at all times and be able to withdraw access immediately from any device
- Secure all devices when not in use through, locked cabinets or in a secure, access restricted room
- Never leave remote access devices or equipment unattended
- Where a system requires a PIN number and a VPN *'security token'*, store both separately and restrict access to them
- Ensure that a virtual private network (VPN) or Microsoft Remote Desktop Connection is used for all remote access connections
- Ensure that all devices used for remote access require a username and password
- Activate and keep updated effective anti-virus software, malware and a firewall
- Destroy remote access devices once no longer in use, by following the ***Data Retention Policy*** protocols

5.2 OFF-SITE WORKING

It is not just remote access that can pose an additional security risk to the Company and the information retained by us. Where employees are permitted to work from home or off-site (*e.g. on client visits or other service provider buildings*), this can also require taking information assets off-site, such as paperwork, reports, emails etc.

Company laptops are provided to ensure that employees can securely access relevant data remotely. Hard copy information should not be removed from the Company premises and instead this needed be scanned and accessed via Company laptop.

On rare occasions, where employees have no alternative but to take hard copy information off-site (e.g. papers for court where use of laptop may not be permitted) this will require written authorisation from Management. If approved, this is required to be in a locked case

Copyright © 2022 | Disability Positive

during transit and to be in a secure, locked cabinet whilst at home. Hard copy information must be kept on the person at all times if not locked away and is not to be disclosed to any person without prior written permission.

If the paperwork is no longer required, it must be brought back to the Company for archiving or destruction. All employees are expected to abide by this policy and its rules and guidelines.

5.2.1 USING AND SECURING REMOTE ACCESS

Using a Company device to connect via remote access pose additional security risks and as such are governed by the protocols and guidelines below. The following content refers to all forms of remote access, off-site working and use of external devices.

Secure remote access is generally always achieved through VPN and occasionally via Microsoft Remote Desktop Connection, set up by the IT Support Service and approved by the **Senior Management Team/Chief Executive Officer**.

Where a Company device is used for remote access, this is restricted to only information that is essential for the purpose of the remote working and is configured to the minimum level required to perform the activities authorised for.

Employees are blocked from accessing certain websites during work hours/while connected to the network at the discretion of the Company and use of social media site is forbidden except for work purposes. Users using a Company connection are not permitted to access, share, transmit or store any restricted, confidential or inappropriate material.

Remote devices are assigned to a sole employee and will be remotely wiped if the device is lost, compromised or the employee has their employment terminated (*or resigns*). Any device lost or stolen must be reported to the Office Manager within 2 hours.

6. RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, and support to learn, understand and implement the Remote Access Policy and subsequent procedures. Management are responsible for a top down approach and in ensuring that all staff are included and have the support needed to meet the regulatory requirements in this area.

Copyright © 2022 | Disability Positive