Group Policy Remote Working Policy

1. Introduction

CareTech Group Holdings provides some employees the ability and opportunity to work remotely where this is appropriate to the role. This enables our employees to work smarter, with greater flexibility and efficiency. Whilst clear benefits are recognised by increasing the use of mobile devices and working remotely, we all need to be mindful of the additional security challenges and risks which will present themselves.

2. Purpose and scope

This policy applies to all remote working arrangements. The purpose of this policy is to protect the information assets owned and used by the Company; to protect other services or networks (to which CareTech Group Holdings and any of its subsidiary's is connected) from misuse; and to comply with all regulatory, legislative and internal policy requirements. This policy applies to all employees, temporary staff, partners and any authorised third parties (suppliers and contractors) who have been permitted access to Company data.

This policy is underpinned by risk management and users must be aware of and take mitigating actions to address any areas of risk. The user is responsible for ensuring confidentiality of work information outside the office (aside from information system related risks e.g. damage or loss of information due to malware, virus etc.). Users are responsible for the safe usage and security of equipment, and records and systems in their possession.

3. Remote / Home Working

Remote working may involve paper records or use of electronic devices to access the Company's network. You may only use a corporately managed machine; either owned or authorised by the Company.
Users are reminded that corporately issued Company ICT equipment remains the property of the Company.

Examples of remote working situations include:

- Home working (formal or ad hoc arrangements)
- Working when 'on the move' (e.g. on a train, during site visits)
- Working at rest (e.g. in a library)
- Working from the premises of customers, clients, delivery partners, contractors, or any other organisations.

4. Remote Access

Remote access is where users gain access to the Company network, their accounts, its systems and resources from remote locations. This must be via corporately managed devices, through the use of corporate smart phones, or corporately owned tablets or laptops. In normal circumstances you should not attempt access from personally owned computers or other personally owned devices which are not specifically authorised. Any such attempt is a breach of policy. See section 11 – Business Continuity for exceptions.

4.1. Methods of remote access

You need to be connected to the internet to be able to access the Company network remotely. You may use a home broadband or a public wireless network and a Company corporate device. You may not attempt to access the Company network using a non-approved device as this poses a security risk. The network can be accessed from a home broadband via VPN (Virtual Private Network). You will have to provide your username, and a pass-code.
The VPN will check that the device you are using has the requisite level of anti-virus and that it meets the Company's security requirements. Without this you will not gain access to the network. Should your device be subject to malware or virus attack while you are logged in to the Company network the connection to the network may be dropped and you may be prevented from further access. Contact the IT Services if you suspect this has happened.

4.2. VPN on your tablet or laptop

VPN enables connection to the network using a private, exclusive link. With VPN, privacy is achieved by encryption, so when information leaves a computer/tablet it is encrypted. It is then sent via a private 'tunnel/pathway' across the internet to a recipient computer /tablet where it is de-coded and received. No one can read the data whilst it is being transmitted, or change it in anyway.

5. Information security

Employees working remotely are responsible for ensuring that all Company information (both paper and electronic) is kept confidential and secure to prevent access by a third party. Even though you are working in a different environment and aren't in the office, you are still required to adhere to all Information Management policies. Some key principles and guidance, specific to remote and home working are outlined below.

- For home working it is recommended that the work area of the house should be kept separate from the rest of the household.
- Always lock your laptop when leaving it unattended
- When leaving the house (even for a short period), your laptop must be shut down and all paperwork put away out of sight.

- Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor, and paper record kept separate from valuables.

5.1. Confidentiality

- Never leave information accessible to other people e.g. family members, visitors, or members of the public.
- Paper files must be put away in a secure cabinet when not in use in the home.
- Paper files should not be stored in the home for any longer than is strictly necessary.
- Where printing facilities are available to you, ensure you do not leave papers lying on the printer and always clear paper jams so as not to inappropriately disclose information to others.
- Take care when making or receiving phone calls when working remotely. Be aware of what others close by may overhear.

5.2. Electronic storage

- Do not email or divert emails to a personal email address in order to work on them remotely.
- Do not create or attempt to transfer Company data on to any personal electronic device.
- Do not use USB data sticks, CDs or other removable media as portable temporary storage for electronic files and documents unless they have been appropriately encrypted.

5.3. Taking paper records out of the office

- Confidential documents/materials or documents containing personal information, must not be taken out of the office without specific authorisation from a line manager. Taking paper records/hard copy material off-site should only happen when it is absolutely essential to do so and there is no alternative method for accessing the information or undertaking the work.
  Records should not be taken off-site just because it is convenient to do so.
- Where papers records/hard copy material have to be taken off-site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed and, where possible, data should be anonymised.

5.4. Data and devices in transit

- Always shut down your device when in transit (even when only travelling for short journeys), to ensure encryption is engaged and the device is properly protected.
- Don’t leave bags or cases containing paper files / tablet visible in a car; if it is unavoidable to store paper records/hard-copy material in a car, lock them in the boot.

- Never leave your device or papers unattended on view in a vehicle. If you do have to leave the device in a vehicle it must be locked in the boot.
- When travelling on public transport keep your bag/case containing Company assets close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of theft or the misplacing of the item.

6. Working in public locations

- When work is required to be done in any public environment care should be taken to ensure that no bystander could overlook any information displayed on the device or any user input (especially passwords).
- The security and confidentiality of data and equipment must be considered at all times.
- Working in crowded locations (coffee shops for example) is inadvisable, and it is not recommended to access personal data unless absolutely necessary.

7. Network access overseas

Access to the network when overseas: if a situation arises in which users need to take their device out of the UK they must first check with IT Services and the Data Protection Officer if this is appropriate, as it may put Company information and the network at risk.
Some countries are banned from connecting to Public Services Network connected networks. Certain countries may confiscate encrypted devices on entry and/or force a user to enter passwords and bypass security. Confiscated devices may not be returned.

8. Responsibilities and liability

Employees

- Must ensure they always have line management approval to work remotely. The exception to this is Social workers that are home based that do not require line-management agreement.
- You are responsible for adopting appropriate and necessary security measures; ensuring that all information (both paper and electronic) is kept confidential and secure to prevent access by a third party.
- Whilst working with Company data remotely, you are required to abide by all Company policies to ensure information is appropriately protected.
- You are responsible for identifying to your line manager any concerns with work processes or other local arrangements that prevent you complying with this or any other policy. Line managers are responsible for ensuring that users are supported in complying with this policy.

Line Managers

- You are responsible for ensuring your team members have appropriate mechanisms in place to minimise the potential loss/damage of Company paperwork/documentation whilst working remotely.

- You may need to agree that the provision of additional equipment will be necessary e.g. fire and tamper proof boxes, lockable filing cabinets or privacy screens for mobile devices, to ensure areas of risk are mitigated.

9. Data incidents

The loss of a Company owned device, such as laptop, iPad, tablet or smart phone, or a loss of paperwork whilst working at home or remotely must immediately be reported to:

- Your line manager
- IT Services
- Data Protection Officer
- Divisional manging Director
- The police (obtain a crime reference number from the police, as this will be required for claim purposes)

Timeliness of reporting is vital to ensure measures are put in place to contain and mitigate any security risks or data loss. Every incident must be reported, logged and investigated as soon as it occurs.

10. Insurance

The Company has Employers and Public Liability Insurance arrangements that will cover remote working in the same way as other employees.
Users shall not incur any liability provided that they take reasonable care of the property.

In the event that you may be working from home under special measures, such as a pandemic situation, and for longer than usual, we recommend that you check your home insurance policy to ensure adequate cover is in place.

11. Business Continuity

On a day to day basis the use of personally owned equipment or personal email accounts for Company business is forbidden. If working remotely is required on either a regular or ad hoc basis this should only be conducted on Company equipment.
However, during business continuity incidents such as building failures or extreme weather it may be accepted that some Company business could be conducted on personal equipment. Line Managers must discuss these requirements with IT Services and **seek appropriate sign-off** as and when needed.
Personal information must only be processed when absolutely necessary. Sensitive personal data (as defined by the General Data Protection Regulation 2018, such as medical or equalities information) should never be sent to or processed using non-Company provided equipment.

Any use of personal email accounts for business continuity purposes should copy in your work account to ensure that the Company has an appropriate record of its business.

Company data must be deleted from personal equipment and email accounts as soon as the necessity to use personal equipment is over.

It is expected that users will prepare for expected events such as tube strikes or forecast bad weather and take equipment home with the approval of their line manager if it is expected that attendance at work would not be possible.

12. Special Measures

In the event of unforeseen situations that affect our business, such as the recent COVID – 19 pandemic, it is possible that working remotely may increase for a large number of our employees. In this scenario, certain parts of the guidance of this policy may be subject to change.

In view of remote working, as a Company we are looking to the latest ICO guidance on this matter, as follows:
Data protection is not a barrier to increased and different types of remote working. During the pandemic, employees may work remotely more frequently than usual and they can use their own device or communications equipment. Data protection law doesn't prevent that, but employees must consider the same kinds of security measures for remote working that would be used in normal circumstances.

13. Policy Review

This policy will be reviewed on an annual basis or sooner as is required e.g. where there are changes in legislation, or recommended changes to improve best practice