COVID-19 Personal Device Usage Policy

Wedge has adopted this Personal Device Usage Policy to assist users to work remotely during the public health emergency.

By signing this policy, you agree to the terms and conditions therein.

Protecting privacy and security are of paramount importance and is part of every Wedge employee's responsibility.

- Wedge is temporarily permitting you access to our network through a secure link on your personal device. This link is a direct connection to our network and can expose our network to security risks if the following precautions are not taken:
    - All antivirus on your personal device must be up to date
    - Only connect through secure internet connections. Insecure connections include (but are not limited to) "hot spots", public WiFi (e.g. Starbucks).
    - Be mindful of the sites you visit on your personal device while connected to the Wedge network. If virus or malware infect your personal device and you then connect to our network, you are exposing protected information to that virus or malware.
- You are not to share access links or access information with others, including current Wedge staff.
- You are not permitted to store any client information on your personal device. This includes capturing screenshots, exporting reports from the health record, using personal email to transfer client information, or writing notes on your personal computer to later transfer to Wedge network.
- Do not permit anyone access to your personal device while you are logged into the Wedge network.
- You must sign out of the Wedge network when you are not working.

In accepting the use of a remote connection, I agree to the following conditions:

1. I understand that I am responsible for the protection of confidential client information.
2. I will only use the Wedge network for Wedge Recovery Center related purposes.
3. I will notify IT Department, Compliance Officer, and CEO of any malfunction or suspicious activity during my remote use.
4. I attest that the device I am using is my personal device and is not used by anyone else.
5. I will not allow my personal device to be used by an unknown or unauthorized person while granted remote access to the Wedge network.
6. I will abide by the Wedge Recovery Center Acceptable Use, Information Security, and Portable Data Device security policies as published in the company folder
7. If my personal device is lost, stolen, or damaged, the incident must be reported to the Wedge IT Department, Compliance Officer, and CEO immediately.
8. If confidential client information is disclosed or exposed, and it is determined to be caused by my negligence or intentional misuse, I will assume full responsibility for my actions.
9. I am aware that any breach of these policies may render me liable to disciplinary action under the Wedge Recovery Center procedures

User Printed name: _____ User Title: _____

Signature: _____ Date: _____

Witness: _____ Date: _____

V1.2 4/2020