

Do's and Don'ts – New Rugged Laptops (Dell Latitude 5430)

Introduction

Welcome to the new SevernSide mobile device for home visits! We are excited to introduce the **Dell Latitude 5430 Rugged Laptop**, which has been chosen for its reliability and durability, replacing the Panasonic Toughbooks.

This device was selected because it offers:

- **Build and Durability:** Engineered to withstand extreme temperatures, dust, vibration, and shocks. It carries an **IP65** or **IP-53** rating for water and dust resistance.
- **Customisation and Expandability:** Features customisation options for storage, RAM, and processor configurations.
- **Display and Usability:** Equipped with a Full HD (FHD) display for clear visibility.
- **Weight and Portability:** Lighter than some Toughbook models, enhancing ease of transport.
- **Battery Life:** Delivers strong battery performance, suitable for long shifts.
- **Security and Connectivity:** Aligns with BrisDoc's digital strategy, ensuring enhanced integration and security.
- **Cost Efficiency:** More affordable than Panasonic Toughbooks, offering a cost-effective solution.
- **Support and Warranty:** Supported internally by the BrisDoc Digital Team, reducing support times.

How to Manage the Dell Rugged Laptop

1. Power Management

- **Power Down When Not in Use:**
Co-owners must switch off the device when it is not being used to:
 - Increase device security.
 - Preserve the laptop's lifespan.
 - Avoid wasting SIM data.
- **Battery Charging Guidelines:**
 - Co-owners must power down the device when not in use:
 - To increase Security of the device,
 - To preserve the lifespan of the Rugged Laptop
 - Stop incurring waste of Sim Data.
 - Once the Rugged laptop is fully charged (Green light is off), Co-owners or Clinicians must not leave device plugged in. Batteries can swell if constantly overcharged, reducing its lifespan.
 - Co-owners or Clinicians must not charge Rugged Laptop in Electric Vehicle unless battery is at 10% or less.

- The battery life for the Rugged laptop is considerably better than the Panasonic Toughbooks, it most likely will last an entire shift or until it is back to base, where it can re-charge quickly.
- Not all Electric Vehicles are the same. BrisDoc's are not designed to have continuous or regular discharge from additional peripherals such as Laptops. This can cause damage to its own battery, fire or invalidate the insurance. Don't test the theory.

2. Battery Management in Electric Vehicles

- **Charging in Vehicles:**
Do **not** charge the laptop in an electric vehicle unless the battery is at **10% or lower**.
 - BrisDoc's electric vehicles are not designed to handle regular or continuous discharge from peripherals such as laptops. This can:
 - Damage the vehicle's battery.
 - Pose a fire hazard.
 - Invalidate the vehicle's insurance.

3. Battery Life Expectancy

The Rugged Laptop's battery is significantly better than that of the Panasonic Toughbooks. It is likely to last an entire shift and can be recharged quickly back at base.

4. Security and Device Handling

- **BitLocker Encryption:**
The laptops are encrypted with a BitLocker code for enhanced security.
 - **Do not write down** or store the code near the device.
 - The code will be changed every six months by the Digital Team. Co-owners must contact the Shift Manager for the updated code or if the current one is forgotten.
- **Tampering with Settings:**
Co-owners must **not** change any settings or tamper with the device or its applications. Such actions will be considered an act of **vandalism** and could result in **disciplinary action**.
- **Issue Reporting:**
If any issues arise with the laptop or its applications, **log the issue** with the Shift Manager and raise a support ticket with the Digital IT team.

5. Device Usage Guidelines

- **Intended Use:**
These laptops are intended solely for use within the **IUC Service**.
 - Do **not download** or install any additional software on the device.
 - Colleagues must not change any settings or tamper with the device or applications. Such actions will be deemed as an act of vandalism and will result in Disciplinary action.

6. Device Monitoring and Maintenance

- The Rugged Laptops will undergo **regular maintenance**.
- The Digital Team will perform **ongoing monitoring** for security threats and to ensure compliance with usage policies.
- For transparency, the Rugged Laptops are installed with BrisDoc's cyber tooling, which will track activity as well protect from threats. Should an incident occur device usage will be audited by the Digital Team.

7. Physical Handling Instructions

- **Carrying and Transporting the Device:**
 - Always use the built-in handle when transporting the laptop to prevent accidental drops.
 - When in transit, ensure that the Rugged Laptop is safely stowed to not cause damage or injury to occupants, the vehicle or the device itself.
- **Cleaning and Maintenance:**
 - To clean the device, use a soft, lint-free cloth and mild cleaning solution.
 - Avoid vigorous cleaning of keyboard with Clinnell Wipes.
 - Avoid spraying liquids directly onto the laptop; instead, dampen the cloth slightly.
 - Ensure all ports and openings are covered when cleaning to prevent moisture from entering.
- **Storage and Protection:**
 - Switch off and store the Rugged laptop in a secure location when not in use.
 - Avoid exposing the laptop to extreme temperatures, prolonged sunlight, or excessive dust and moisture.
 - Do not leave the Rugged laptop in a vehicle unattended.
 - Do not leave the Rugged laptop switched on and left unattended when with a patient or in the vicinity of non BrisDoc colleagues, even if it's just being left for a short time. Lock the screen at a minimum.

8. Maintenance Schedule

- **Regular Checks:**
 - Device audits and maintenance checks will occur every month. During this time, the Digital Team will assess the hardware, check for software updates, and conduct any necessary report of its use.
 - Prior to scheduled maintenance, the Ops Team will receive advanced notification, and if viable a back-up device to be left in its place.
- **Self-Check Reminders:**

- Prior to visits, it is recommended that the driver perform pre-checks of the device such as, it has Internet access and can launch the Remote Clinical Application during start of shift checklist, if rebooting does not resolve the issue notify the shift manager immediately of connection issues.
- Co-owners should visually inspect the device regularly for any signs of wear or damage, such as loose components or scratches on the screen.
- Report any issues immediately to Shift Manager and Digital IT for early intervention.

9. Reporting Issues

- Any issues with the Rugged Laptop or its applications must be logged with the Shift Manager and a support ticket logged with Digital IT.

10. Emergency Protocols

- **Loss or Theft:**
 - If the Rugged laptop is lost or stolen, report it immediately to Shift Manager.
 - The Shift Manager and Digital Team will make secure or remove sensitive data on the device.
- **Data Protection:**
 - Avoid storing sensitive information directly on the laptop's hard drive/ desktop.
- **Password and Access Management:**
 - Use strong, unique passwords and avoid sharing them. If a password is compromised, report it immediately to IT for a reset.