Tamper Prevention Inspections for Payment Card Terminals

These checklists are intended for all contactless payment terminals. All terminals should be inspected for tampering before every use by following the items listed below. For the best results, view this checklist in the Desktop App.

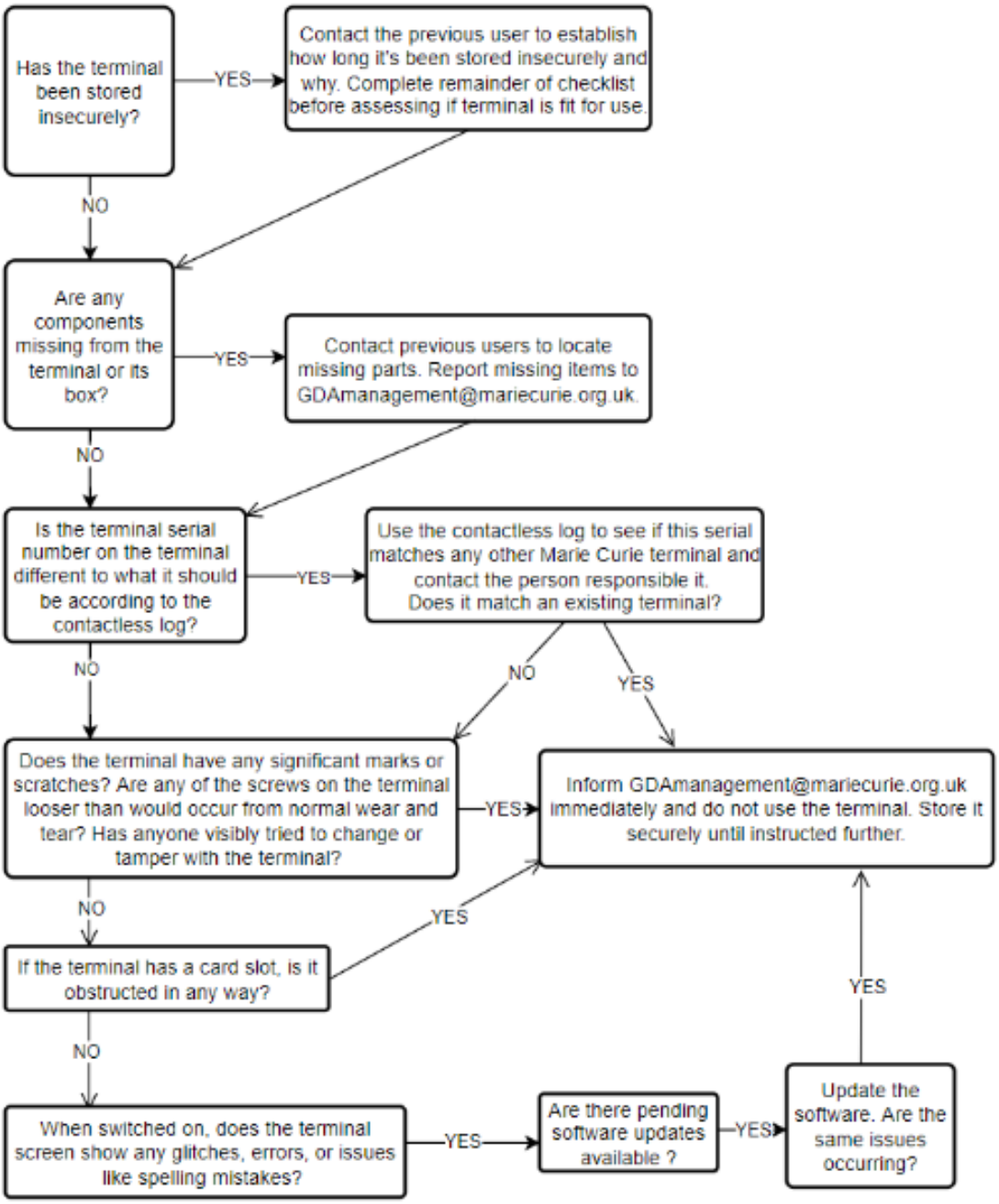
Tamper check	**Info**
Name of person completing tamper check	
Date of tamper check	
Location of terminal	
Type of terminal (eg. Liberty Pay Payter)	
Terminal serial number	

Tampering Checklist	
Has the terminal been stored insecurely?	
Is the terminal serial number different to what it should be?	
Does the terminal have any marks or scratches?	
Are any of the screws on the terminal loose?	
Has anyone tried to change or tamper with the terminal?	
When switched on, does the terminal screen show any glitches, errors, or issues like spelling mistakes?	
Are any components missing from the terminal or its box?	
If the terminal has a card slot, is it obstructed in any way? To test this, insert a non-payment card (drivers license, library card, or similar) to see if it goes all the way into the terminal)	

End of day checklist	**Tick to indicate completion**
The terminal has been fully charged	
All transactions for the day have been uploaded via WiFi or 4G.	
The terminal has the latest software	
The terminal and its components (instructions, charger, etc) have been returned to its box	
The terminal is powered off	
The terminal is locked away securely	

Problem with your terminal?

If any of the tamper checklist questions were answered with ‘Yes’, please see the below flowchart



All Paya terminals can be remotely de-activated after a theft or misplacement. If you suspect your Paya unit has been tampered with you can call reach their customer support line on 0333 123 1243. Please also notify GDAmanagement@mariecurie.org.uk

All GB mini devices are built with an anti-tamper mechanism to prevent misuse i.e someone gaining entry to the device to install card skimming hardware / card cloning software, if the tamper mechanism is triggered, the device is rendered unusable and cannot be repaired. “Tamper Detected” will be displayed on the screen if the tamper mechanism is triggered.