

Do you know where your organization's sensitive cell phone data is going?



## Ensuring Your Organization's Wireless Data is Protected

e-Cycle Whitepaper



e-Cycle LLC  
4105 Leap Road, Hilliard, OH 43026  
Phone: (614) 210-1120  
Toll-free: (877) 215-5255  
GoGreen@e-cycle.com  
www.e-cycle.com

## Contents

Executive Summary.....	2
Responsible eCycling.....	3
Comprehensive Data Protection.....	4
Shipping and receiving.....	4
Sorting, Destruction and Recycling.....	4
Internal Security Procedures.....	5
Summary.....	6

## Executive Summary

Wireless recycling is a growing concern for businesses and organizations. Each year, more than a billion wireless phones are retired worldwide. Yet surprisingly, only 10% of these phones are recycled. Organizations have a responsibility to ensure their wireless devices are handled in a way that doesn't jeopardize sensitive information or contaminate the local environment.

The average smartphone can contain 4-8 GB of data. Like laptops, modern wireless devices are filled with confidential personal and professional information. Passwords, emails, work documents, photos, text messages and contacts are all stored on the device and can present a potential security risk if this information is not removed. Organizations need a policy in place to ensure they are not vulnerable to security breaches.

Despite this, many organizations do little to protect themselves from these threats – even when they may have hundreds or thousands of devices at large. Often, sensitive information remains even after the user has attempted to delete all data from the device. Ensuring the data is properly removed requires a rigorous process and specially-trained technicians. Faced with these realities, organizations have a new responsibility to get smart about how they retire their obsolete devices.

e-Cycle is the global leader in wireless buyback and recycling. We partner with thousands of organizations to provide a structured, secure and profitable solution to an increasingly important issue. We have recycled or resold more than four million cell phones since 2005.



**Resale value**  
A typical smartphone can retain a majority of its original retail value after 12-18 months.

**Hazardous waste**  
Toxic materials inside wireless phones and other electronic waste comprise more than 70% of pollutants in today's landfills.

**Sensitive data**  
The average wireless device contains 80 MB of potentially sensitive data that comprise a very real security risk.

## Responsible eCycling

Every organization should have a buyback and recycling plan to ensure the greatest return on telecom investments. Most organizations retire their wireless devices within 18-24 months. At that stage, these devices can retain a significant percentage of their retail value. However, cell phones that are not properly retired may expose confidential data when they are resold on the secondary market or harm the local environment through improper recycling and disposal.

Here is an overview of the e-Cycle process:

### Recycle

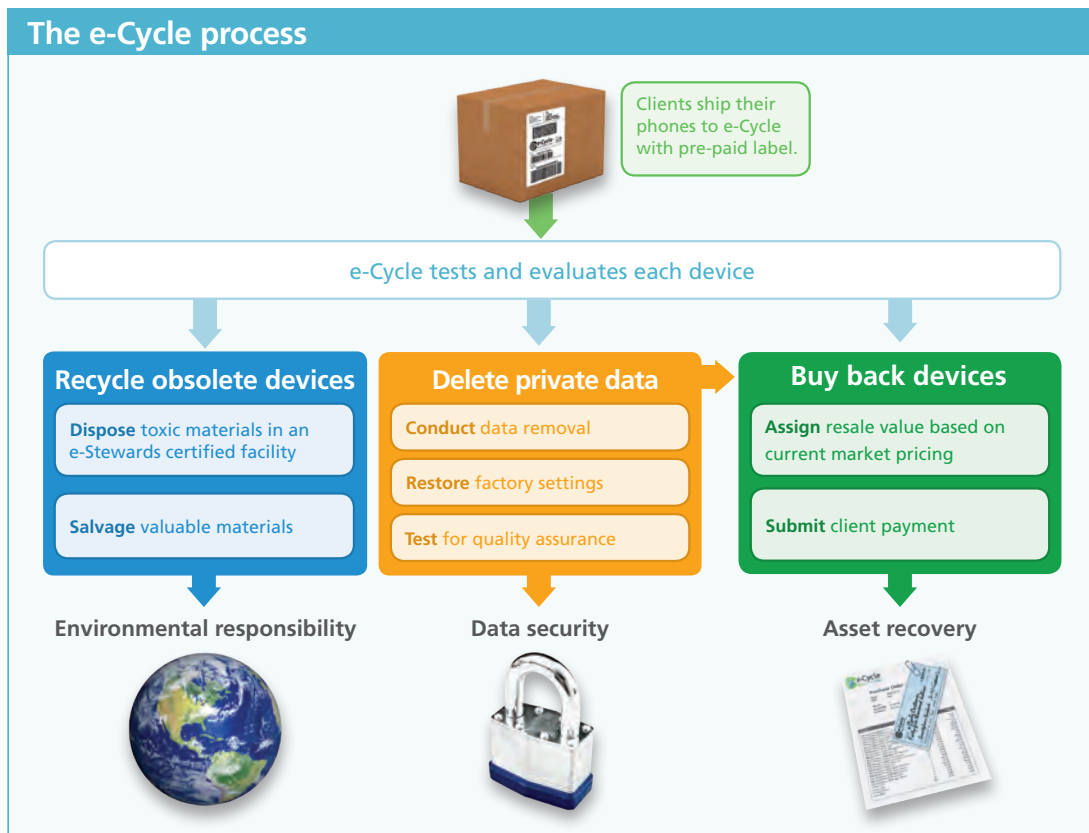
Our specialists evaluate all equipment to assess its resale value. Phones that are non-functional, as well as accessories, are sorted out to be destroyed. Every battery is removed and sent to an e-Stewards certified facility to make certain its toxic materials do not end up in a landfill. The core technology, including the motherboard and all wiring, is shredded and melted down so that the precious metals can be reused.

### Recover

Our clients send us their wireless devices using pre-paid shipping labels provided by e-Cycle. They receive a check for the phones that retain their resale value and are in working condition. e-Cycle uses the latest market pricing to determine the value of the equipment. Each of our clients receive a full inventory report detailing the make, model, value and condition of each phone. Our clients receive payment in 30 days or less after their shipment arrives to our facility.

### Protect

All functional phones are put through a comprehensive data removal process to make certain that all private information is permanently deleted. We also test every phone for active lines and inform the client if any are found to protect against unintended fees. After restoring the factory settings, our quality assurance team rechecks every device to make sure the data has been completely cleared of all confidential information.





## Comprehensive Data Protection

End-of-life cell phones should not be unwisely viewed as scrap, a simple donation or a hasty recyclable. They are archives of confidential data. If a cell phone or smartphone is dumped, donated or refurbished and resold improperly, any remaining data could be accessed.

e-Cycle provides the industry's most thorough and secure process for removing corporate and personal data from wireless equipment. For every phone we purchase, we manually remove all private information and restore each device to its factory settings. Our quality assurance team rechecks every device to ensure the data has been cleared.

Our high-security work environment and processes have been meticulously designed to maintain the utmost protection. For example, e-Cycle is Department of Defense compliant on all data security compliance regulations for BlackBerry phones.

### Shipping and Receiving

Prepaid FedEx labels are provided to e-Cycle clients to ship their devices.

Intake is done each morning as delivery service shipments are received. The packages are counted and registered with the intake supervisor.

- The name of the shipper, the number of packages received and the condition of the packages are recorded.
- If a shipment contains a damaged package, a photograph is generated and submitted to the e-Cycle customer service representative who contacts the client immediately with detailed information.
- The packages are then sorted, opened and checked against the company inventory list (if included). The sorting staff counts each shipment four times to verify accuracy and checks for any special processing requests which may be applied to the shipment.
- Any discrepancies between the supplied inventory list and the official count by the sorters are noted and sent to the customer service representative.
- Notifications of discrepancies are communicated to the client and the final disposition is determined.
- Cleared shipments proceed to final sorting and initial inventory processing.

### Sorting, Destruction and Recycling

For the purpose of the information below, the following terms are defined as follows:

- "Destroy" or "destruction" is rendering a device unusable through destruction techniques including, but not limited to, disintegration, incineration, pulverizing, shredding and melting.
- "Dispose of" is the act of discarding the mobile device with no other use being considered.
- "Recycle" is the act to reuse the mobile device, whether via sale or donation by the vendor.
- "Wiped clean," "scrubbed," or "erased" is rendering the device data unreadable and inaccessible.

After receiving shipments from our clients, devices are either destroyed or recycled. e-Cycle does not dispose of any devices. Devices to be destroyed are separated from devices to be recycled.

A purchase order is provided for each shipment received by e-Cycle. The purchase order (PO) includes the number of recycled and disposed of devices by model and quantity. The PO also details a listing of devices that did not pass the quality assurance process and the reason for the failure, as well as the phone number of any devices with active lines.

### Devices to be destroyed

End-life-devices that are no longer functional are destroyed.

- All destroyed devices are shredded on site at e-Cycle's recycling facility the day they are received.
- Destroyed devices have their battery removed, are counted to provide an aggregate number to our client and then shredded.
- SIM/SD or other data-storage cards are shredded in a specially-designed device. SD and data-storage cards are shredded upon receipt. SIM Cards are shredded after testing for activation that day.
- All end-of-life wireless phones and accessories are sent to Reldan Metals refining facility (EPA ID number PAD002365849) in the United States to ensure its toxic materials do not end up in a landfill.
- There is no way to track a shredded device back to its original owner.

# Ensuring Your Organization's Wireless Data is Protected

e-Cycle Whitepaper

## Devices to be recycled

All recycled devices are processed by highly trained data security specialists. To ensure all personal data has been removed or destroyed, every device is retested by e-Cycle's quality assurance department.

Devices to be recycled are received and separated from the devices to be destroyed. The devices targeted for recycling are inventoried by model, quantity and ESN or IMEI number unless otherwise directed by the client.

- After sorting, devices to be recycled are stored in a limited access, lock-down facility and staged for data deletion and functional testing.
- Individuals that have access to the storage facility are scanned each time they leave the building by a airport security scanner operated by a full time security guard.
- Reusable phones are put through a comprehensive data removal process to ensure that all proprietary applications and corporate/personal information is permanently deleted and wiped clean.
- We also test every phone for active lines, and recycle any that are found to be still active (see "Devices with active lines" below).
- Once the testing and data-deletion process is complete, the devices go through an extensive quality assurance process handled by a separate e-Cycle department. All of the devices are double checked to make certain they are completely wiped clean.
- Some devices may be outdated or damaged to an extent that data security is at risk. All such devices are physically shredded on-site the day they are received.
- The scrubbed devices are then entered into e-Cycle's inventory system for resale to trusted overseas partners. Shipments are made in plain generically labeled containers.
- A certificate of device destruction is also available upon request.

## Devices with active lines

Devices found to have active lines with a carrier are data security problems. The corresponding information is sent to the client, including the active phone number(s) for de-activation. All active devices are physically shredded on-site the day they are tested.

## Internal Security and Procedures

In order to uphold the highest data-protection standards in the industry, e-Cycle employs rigorous hiring practices and internal security procedures to ensure the wireless devices are protected from theft and data breaches. These measures are strictly enforced. It is imperative that our security measures meet the standards of our clients.

### e-Cycle hiring practices

Every new hire at e-Cycle must undergo a thorough criminal background screening before entering into employment. e-Cycle utilizes Secure Check to conduct a five-point background check, including SSN Trace, Past Address History, National Criminal Database, BCI Fingerprint, and Criminal County 7 Year. **A candidate who shows any prior conviction for a misdemeanor or a felony is prohibited from entering into employment with e-Cycle.**

### Facility security and procedures

Every employee or visitor entering or exiting the e-Cycle facility is required to follow strict security procedures in order to maintain a protected working environment. These procedures include, but are not limited to:

- **On site security guard** - A full-time security guard is located in the front lobby to ensure all security procedures are strictly enforced. No one is permitted to leave the facility unless a security officer is present at the security desk.
- **Metal detector** - All employees and visitors must exit the facility through a metal detector to make certain that no cell phones, USB devices, data cards, or other data-storage devices leave the building. Any unauthorized cell phone or data-storage device discovered upon exiting the facility is confiscated and result in strict disciplinary or legal action.
- **Cell phone registration** - Any employees or visitors carrying a personal cell phone is required to allow e-Cycle security to record the cell phone's ESN/IMEI/MEID/etc. numbers before they leave the lobby area. All phones must be verified before leaving our facility.
- **Limited access** - No visitors are allowed to enter the e-Cycle facility without an appointment made at least 24 hours in advance. It is restricted for visitors or employees to enter the warehouse or operation areas without an escort. The e-Cycle facility entrance and warehouse is locked down with electronic doors. Everyone must pass security area to enter the building.

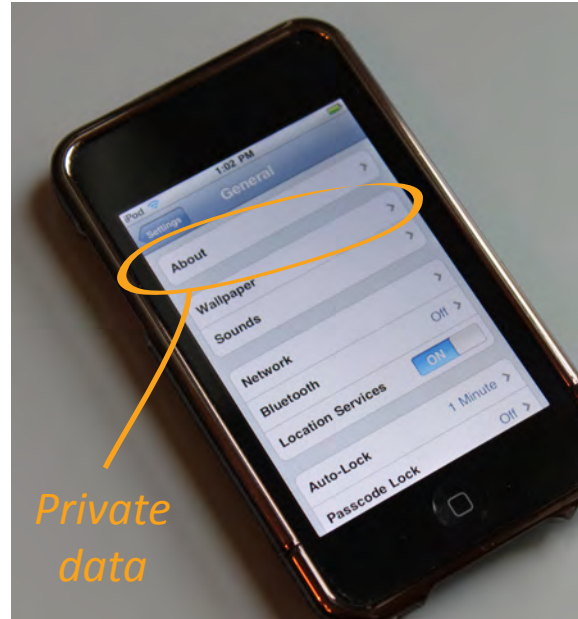
## Summary

With electronic waste and data security presenting such a growing problem, organizations need to put policies in place that specifically address wireless recycling. This is a vital sustainability concern and has been the focus of increasing environmental regulations.

To do this effectively, they need a comprehensive policy that reflects the gravity of these issues and a serious, ongoing program to put that policy into action. Most of all, they need a partner they can trust.

e-Cycle is privileged to partner with leading organizations in all major industries including financial, educational, healthcare, government, retail, manufacturing, and telecommunications. More than 6,500 organizations have utilized e-Cycle's wireless asset recovery program.

We are the trusted buyback and recycling partner for a majority of the top Fortune 500 companies in the United States.



© 2010 by e-Cycle LLC.

All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of e-Cycle LLC.