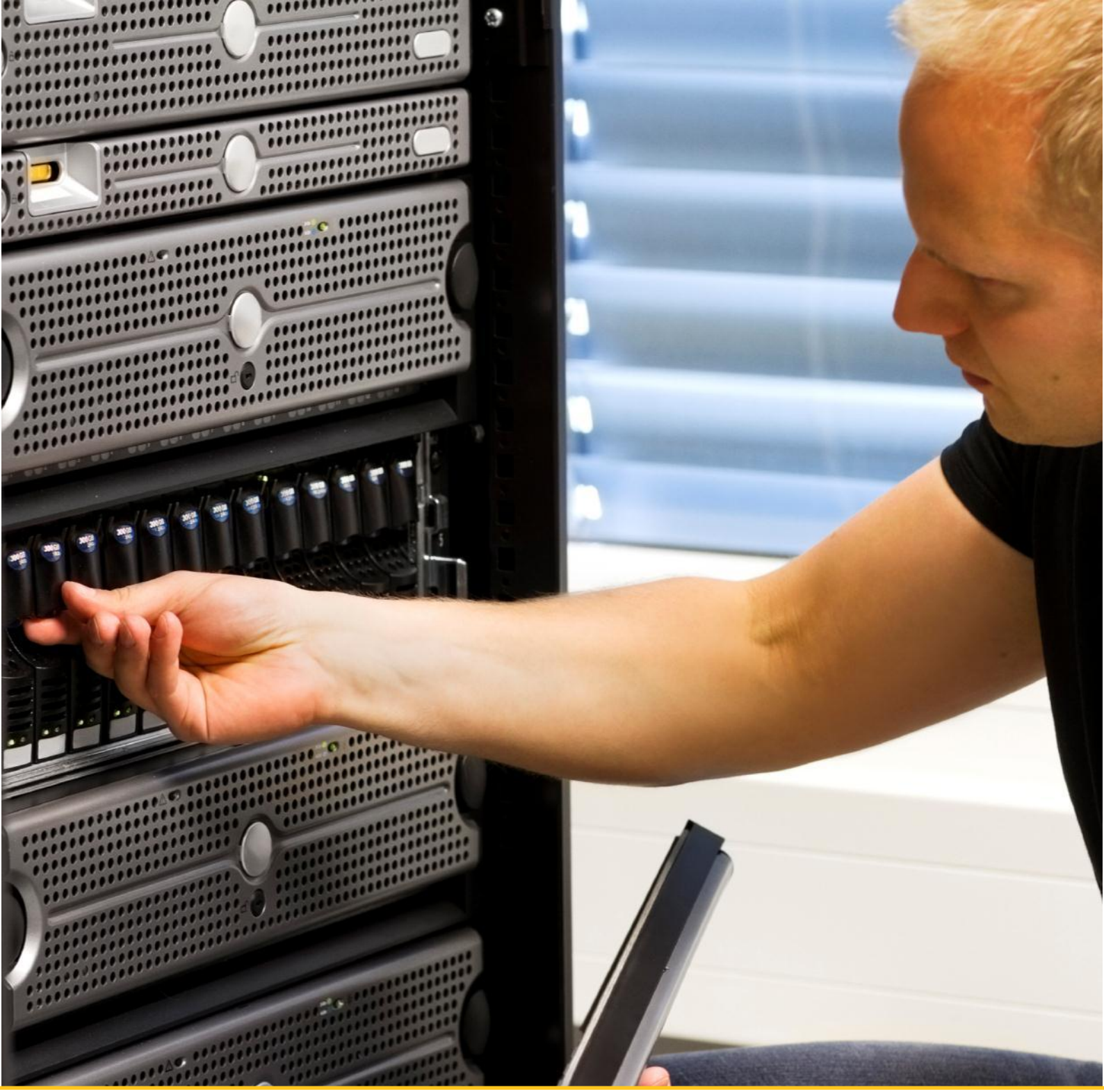

SIMS LIFECYCLE SERVICES

IT ASSET DISPOSAL

Version 2.0
22/01/2013

Contents

1.0 What is IT Asset Disposal?

Information Technology (IT) is now indispensable to the modern organisation. It maintains data on employees and customers; holds and provides analysis of accounts; designs and stores blueprints on technology and communicates a company's strategic objectives. In short it reaches into every corner and aspect of a company and its culture. After employees, IT is responsible for a company's greatest asset... information.

So it is important for an IT Director to manage this technology, to ensure they are up to date with the latest software and hardware that means the information and communications of a company are handled as efficiently as possible.

Inevitably this means that IT equipment becomes redundant or surplus to the company's needs, due to it being superseded or through its failure. IT Asset Disposal believes that this equipment is still an asset of value to the company due to:

- The information it contains
- The intrinsic re-use value of the equipment or its components
- The potential value of its constituent materials
- Meeting the company's corporate social responsibility objectives

Sims Lifecycle Services works with clients to ensure the most appropriate strategy is found for these electronic assets. Examples of core strategies are shown below:

- Gain maximum value from the equipment through compliant and safe reuse, redeployment and disposal options
- Ensure the complete destruction of data or hardware under maximum security
- Demonstrate the meeting of Corporate Social Responsibility objectives through obtaining valuable management information on assets recovered, their condition, their disposition routes and the subsequent benefits to a community project or the environment

1.1 The Importance of Responsible IT Reuse and Recycling?

"Greening the Public Sector", a case study by the UK's Technology Trade Association, states that IT produces 2% of the world's total carbon footprint. However, it also demonstrates IT as the primary player in reducing our overall carbon footprint. The report cites a Local Government study in Sunderland, which found that increasing IT's specific footprint by 4,000%, reduced the overall footprint of the Authority by 30%. In support of this, McKinsey estimates that 7.8 billion tonnes of CO2 could be saved by the use of IT in buildings, power, transport, manufacturing and teleworking. Strategic development in the IT marketplace supports this, with new technology being "greener" and often being developed to support sustainable activities.

Beyond carbon footprint, IT requires a disproportionate amount of resources to manufacture. For instance, a standard desktop computer requires 1.8 tonnes of materials to manufacture. Of the constituent materials it contains, some, are highly valuable precious metals and others include certain rare earth metals; now included in the sustainable development proposals of a number of Governments. These "critically important materials" have various government strategies for securing future sources of the commodity.

Technology also contains hazardous materials, which if not treated correctly at the end of their lives, have the potential for serious environmental and human harm.

Due to this, there is a growing trend in global legislation to improve electronic equipment's carbon lifecycles in manufacture and use, reduce hazardous materials used in their manufacture and ensure the equipment is being recycled to certain standards at the end of its life. Other legislation is driving sustainability development which demands the latest technology to support it.

The fundamentals of this legislative strategy are admirable, but in reality they have caused two challenges that must be faced:

Shortened Lifecycle – in the race to achieve greener IT equipment, the IT lifecycle may well be shortened creating a short term increase in electronic asset retirement.

Market Exploiters – legislation has created a new market place for the recovery and recycling of electronic assets. As with any new marketplace this will attract both professional companies and opportunists who are out to exploit the legislation for short term profits.

Meanwhile the problem of redundant IT keeps growing. In 2008, a Gartner Study estimated that over 2 billion computers had been manufactured. Gartner also believed that in the year 2008, 180 million PCs (16% of PCs in use) would be replaced. And a fifth of those would end up in landfill with no regard to the loss of resource or impact on the environment... 36 million PCs.

This resource challenge is even greater when you consider the growth of personal devices. In 2011, Gartner estimated that 1.7 billion mobile phones were shipped, 11% more than in 2010. Of these 490 million were even more resource intensive, Smart Phones. Meanwhile, IDC estimated 122 million Tablet computers were shipped in 2012, growing to 172 million on 2013.

2.0 Data Destruction Methods

The need for data security comes from two drivers, legislation and corporate sensitivity. Research has demonstrated that it is now the number one driver for IT Managers and Directors and large portions of budgets are assigned to maintaining the security of a business' current electronic assets. However, it is only in recent years that attention has turned, deservedly, to the redundant and surplus equipment that a company disposes of.

This attention has mostly been focused on hard drives, but in reality sensitive data can now be found on a number of different types of equipment, as shown in Fig.2.

Items Covered	Risk Exposure
Desktops, Laptops, Servers: Hard drives containing confidential company information.	Deleting does not delete files, reformatting still leaves accessible data.
Printers/scanners/copiers/faxes	Many of these devices now have either an internal hard drive (around 4Gb – 20Gb) or a digital "flash" card (1Gb). This non-volatile memory stores the information on print jobs and is retained until overwritten
Other data storage media CD's, DVD's tapes, USB Sticks	All contain company data that is retrievable
Communications devices – Mobile phones /Tablet Computers /Blackberries /GPS	As above including personal data on bank accounts etc, contacts and emailed documents plus satellite navigation data on home (& other) addresses.
Network equipment – routers, switches	Not company data but do contain network-specific data such as static IP addresses which expose networks to external risk of infiltration
Point of sale, retail debit/credit terminals	May contain personal credit/debit information

Fig. 2. types of electronic equipment and the data security risk they pose

Loss of data can lead to a number of potential issues for an organisation:

Non-compliance with Legislation – unprotected release of information can leave your company at risk from failing in your duty of care. See section 2.1.

Data Breach – Business critical information could be released, unprotected, into the open market. In certain second hand markets, the value of Electronic equipment is now dITated by the quality and quantity of the data it contains, as opposed to its inherent value as a product or recovered materials

Brand Damage and lost credibility – A large degree of high profile press interest is ongoing in association with both breaches of data security and the illegal shipment of an organisation's electronic assets to third world countries, for "recycling" through extremely hazardous methods.

2.1 Legislation Related to Data Security

2.1.1 Copyright

As owners of software licenses, companies have a responsibility to ensure that copies of software are not being passed on outside of the license holder's control.

2.1.2 Data Protection Act

The Data Protection Act (1998) ensures the privacy of personal information stored electronically on computers in the UK. The Act aims to "promote high standards in the handling of personal information, and so to protect the individual's right to privacy".

2.1.3 Sarbanes Oxley (SOX)

This American Act has implications to any companies operating with an American parent. It has peripheral involvement in data security to the extent that Section 302 requires the CEO and CFO to certify that the financial reports are true and accurate, and that there are in existence adequate controls over financial reporting and disclosure. Section 409 requires publicly traded companies to promptly report any changes in financial condition or reporting that might be material to investors. IT security is important under SOX only to the extent that it enhances the reliability and integrity of that reporting.

2.2 Standards for Data Destruction

Data Deletion is also known as Data Destruction, Data Sanitisation and Data Wiping. It is the process of destroying all data that might be housed on an electronic device such as a computer, laptop, printer, hard drive, mobile phone, etc.

Sanitisation is often referred to as being effective for different levels of security. Often terminology is different for different Governments, but figure 3 demonstrates a rough correlation between the standard terminology used to describe these levels of UK security.

Impact Level (IL)	IL Descriptor of Data	Secure Sanitation Level (SSL)	High or low security
6	Top Secret	SSL3	High
5	Secret	SSL3	High
4	Confidential	SSL2	High
3	RestrITed	SSL2	Low
2	Protect	SSL1	Low
1	Protect	SSL1	Low

Fig. 3. A table demonstrating the correlation between different security levels

Data security can be broken down into three areas:

- The security standards relevant to data destruction or hardware destruction
- The security standards related to operations
- The security standards related to people

2.2.1 Data Deletion Security Standards

Software deletion standards in the UK are governed by the CESG (Communications Electronic Security Group) who are the National technical authority for information assurance. They are concerned with creating standards on the deletion of data through software or degaussing.

Currently the recognised standards relevant for data deletion are:

- HMG IA Standard No. 5, Secure Sanitisation of Protectively Marked or Sensitive Information – April 2011, Issue 4.0.

This standard, although UK based, is widely regarded as the highest standard for data deletion in the world.

The CESG has a list of both software products and degaussing products that conform to this standard, and whether these products conform at either the higher or lower levels of security. All products have been rigorously tested to the standard by QinetiQ.

Other recognised standards exist for software deletion, most of which are linked specifically with a particular country or government. Another important one to recognise is Common Criteria Evaluation Assurance Level (EAL) 3+, augmented with ALC_FLR.3. Common Criteria is an internationally acknowledged independent security certification, recognised by governments in 26 countries across Europe, Australasia, Asia and North America.

2.2.2 Hardware Destruction Standards

UK standards for hardware destruction are controlled by a department of the Cabinet Office.

These standards are linked with the premises/business that operates the service offering secure destruction. They look at the systems, processes and infrastructure of that business to ascertain a baseline standard. By default any company saying they can process to Government standards must also operate a quality management system such as ISO9001.

The Government standards also dITate to what level hardware destruction must conform. The standard covers everything from degaussing or granulation through to destruction via burning or explosions! In regards to standards for granulation: essentially, for high sensitivity it requires a method of granulation that can reduce magnetic storage devices to flakes smaller than 6mm in size and solid state memory devices to less than 2mm in size.

2.2.3 Security Standards Relating to People

In the UK, the most basic level of security standards relating to people is the CRB (Criminal Records Bureau) check. After this, the most widely recognised security check for personnel with frequent and uncontrolled contact with secret assets and top secret information is SC (Security Clearance). This includes the following background checks on the individual:

- Involves a basic security clearance check (thorough vetting of CV and identification documents)
- Checks against UK criminal and security records (if appropriate overseas)
- Credit checks

An even higher level of security clearance is Developed Vetting, appropriate for people with long term and uncontrolled access to the most highly sensitive information.

2.3 Data Sanitisation Techniques

Data can be sanitised through three basic techniques:

- Specialist software tools that delete the secure data only
- Degaussing techniques that wipe all information on an IT or media device
- Physical destruction to destroy both the data and the device

2.3.1 Data Deletion through Specialist Software (Magnetic Storage Devices)

When files are written to a hard drive, a pointer is also written in a different area of a drive. Similar in concept to a card file in a library. When files are normally deleted, it is only the pointers (the card file) that are deleted. The files remain un-changed (the books stay on the shelves) until they are eventually overwritten by new data. As such old files, long since thought to be deleted (from the card file) can actually be easily retrieved from the shelves.

Data deletion works by deleting the pointers and all the files in the "library" by over-writing the information on the drive several times with random information. This pass is done several times because the writing arm on a hard-drive is not in a fixed groove like a record; staying on a rough path, as opposed to an exact path. As such, physically, data can still partially exist as the over-writing does not fall exactly over the previous information path. By over-writing several times, you cover more of this "rough" path with the random data, see Fig. 4.

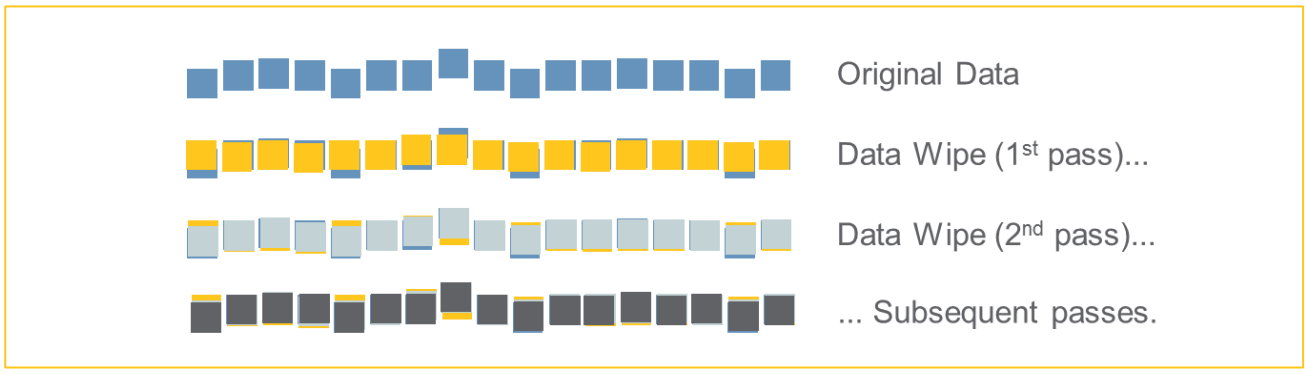

Fig. 4. Demonstrating the data-wiping process through multiple passes of over-writing

The IT Lifecycle Services proposition uses Blancco Data Cleaner (BDC) to securely destroy all information contained on electronic devices such as hard drives. BDC is recognised as the industry leader in data wiping. It is approved to the UK's HMG IA Standard No.5, Secure Sanitisation of Protectively Marked or Sensitive Information – April 2011, issue 4.0, and also with Common Criteria Evaluation Assurance Level (EAL) 3+, augmented with ALC_FLR.3.

2.3.2 Data Deletion through Specialist Software (Solid State Storage Devices)

Solid State Storage devices use a very different technology. Rather than magnetic storage, a Solid State Storage Device (SSD) uses a series of microchips to store and control the access to data. SSD memory is rapidly becoming commonplace due to its low energy requirement and excellent physical size to memory storage ratio. Although ubiquitous on mobile technology such as MP3 players, Smart Phones and Tablets, SSD technology is now regularly seeing use on lightweight laptop computers, also.

The biggest challenge to securing data on SSDs is that there is no common standard to how SSDs work. As such it is very difficult to come up with a software tool that can be guaranteed to securely destroy all information. Although tools now exist to achieve this, none have been ratified by recognised Government bodies, as yet.

2.3.3 Data Destruction (Degaussing)

Another method for destroying data on IT equipment is via a degaussing unit. Memory on equipment such as computers and hard-drives is stored as a series of polarised (positive and negative) magnetic fields. These fields represent 1s and 0s making up specific information in binary code. A degaussing unit exposes the equipment to incredibly powerful magnetic fields which effectively ruin the intricate polarisation of the information, effectively overwriting the data with nothing.

Different IT equipment might have differing capacities to shield themselves from magnetic fields. Without the right level of degausser, there is a chance that the equipment will not be securely sanitised. This measurement of a degausser's power is called the coercivity of the degausser and is measured in Oersteds (Oe).

The downside to this technology is it utterly destroys data held in memory across the whole equipment. So not only will the data held on a hard-drive be destroyed, but so will the intelligence that tells the hard-drive how to work, rendering the drive or other equipment effectively useless.

The degaussing equipment used by Sims Recycling Solutions is capable of HMG IA Standard No.5 sanitisation levels for higher levels of security. However, with modern software sanitisation techniques and hardware destruction, degaussers are becoming less commonly used; partly because there is no definitive "visible" proof to the client of their effectiveness.

Another downside of degaussing technology is it only works with magnetic storage devices. SSDs are impervious to degaussing technology.

2.3.4 Physical Destruction

Physical hardware destruction generally uses a hammer mill, shredder or granulator to reduce equipment to flakes of less than 6mm or 2mm in size depending on the technology. Magnetic devices need granulation to less than 6mm, because the damage inflITed by the initial "cut" creeps beyond this area due to oxidation and thermal damage. SSD technology is more robust and does not suffer the same "creep", within a 6mm area considerable information might be left undamaged. As such granulation for sensitive information is recommended to less than 2mm. Achieving these relative reductions for magnetic or SSD technology meets the required standards for secure destruction, recognised by Government.

Data sanitisation through hardware destruction is suitable for a range of IT and media storage devices such as Hard Drives, Data-Tapes, CD/DVDs, USB sticks, SSD cards, etc.

A final use of physical destruction is for when a client wants to destroy an entire product due to market sensitivities. For example, to prevent goods ending up in a grey market, or to destroy prototypes, etc.

Sims Recycling Solutions performs physical destruction through a number of methods:

- Primary Shredders – with high throughput. These are mainly targeted at high recycling rates which requires larger granulation sizes, but can be tasked to achieve tight granulation requirements
- Mobile Shredder – targeted at achieving Government recognised destruction levels at a client site. So hardware is destroyed before leaving the premises
- Hard Drive Breaker – for remote client facilities, a cost effective solution designed to shatter a Hard Drive platter, making data recovery much more difficult, until transport to a suitable process for further destruction can be achieved

Any granulation or broken material is further secured by the Sims' process. Initially it is mixed with large quantities of other material before being sent through various sorting techniques, including very high powered magnets. This final processing maximises the recovery and refinement of component materials for recycling and also further degrades data recovery potential.

3.0 IT Asset Disposal Services

As previously discussed, the three core strategies for IT Asset Disposal are based on:

- Best Environmental/Social Performance
- Best Data/Hardware protection
- Best price performance

Whilst all three strategies are employed in any IT asset recovery program, achieving excellence in more than one is impossible. For example: Best Data Destruction would require expensive deployment of data sanitisation techniques, impacting on the value recovered from resold equipment. Whereas most cost effective recovery would require the selling of equipment for best value, rather than donation to charity for best social performance, etc.

Whichever strategy is chosen, it is vital to receive comprehensive reports to demonstrate your business objectives have been achieved.

In Sims Lifecycle Services' case, asset reporting is done via a bespoke system called WebView, a comprehensive web-based process control system. It enables the efficient asset management of end of life IT equipment, whilst providing clients with full control and real time reporting of information.

WebView enables clients to have access to their account when required, to book collections of equipment and download specific reports through a secure extranet.

3.1 Online Asset Tracking and Management

When Sims Lifecycle Services' logistics team arrive on site to sanitise and/or collect equipment, they are armed with appropriate collection documentation from WebView. Equipment collected is recorded against this "request" register.

As soon as assets arrive at one of Sims' secure processing facilities, they are received onto WebView and assigned a unique tracking identification reference which remains recorded in WebView tracking each movement of the item whilst in the asset recovery process.

This unique identifier, or tracker, is coded with all the relevant information about the asset, including make and model number, specification, serial number, any asset numbers, origin and condition. WebView automatically identifies and records individual assets for reuse, remarketing or environmentally sound recycling; providing the client with complete knowledge of their asset's disposition route, at any one time. It is possible to set a bespoke route or destination for equipment if required by a client with the WebView "decision tree" system.

3.2 Tracking Data Security

Every data bearing asset entered into WebView has its data completely erased to HMG IA Standard No 5 by using the Blancco Data Cleaner software.

A unique feature to WebView's use of Blancco Data Cleaner is that it is embedded within the tracking software. This brings two advantages:

Firstly- WebView can instantly track whether Blancco has been utilised on an asset, removing human error from the data deletion process. Where hard drive damage does not allow for the platters to be securely sanitised, the WebView process diverts the Hard Drive for physical destruction.

Secondly- WebView can store information on all software being destroyed in the process of deleting data on the computer. This information can be given back to an IT manager who can reclaim software licenses for installation on to different machines, or deletion from their asset register.

3.3 Tracking Resources

WebView tracks a client's electronic assets from collection through the entire asset retirement process on to the final disposition route of the equipment. WebView's client reports are fully customizable, allowing the authorised viewer to specify the detail level and frequency of reporting. This allows the customer to understand the value left in their assets as well as where the assets end up, creating an open-book relationship with your asset management provider.

3.4 Secure Logistics

Technological developments like on-site shredding and remote deployment of software destruction services have reduced the requirement for secure logistics. However for cost effective pick-ups or where the destruction of large hardware items is required, a number of options are available to ensure risk is reduced to a minimum.

Personnel – a driver, by a minimum standard can be CRB (Criminal Records Bureau) checked or higher standards such as SC and DV can be requested.

Vehicles – Secure vehicles can be used to ensure equipment is safely transported. Vehicles can be GPS tracked to monitor and track progress through the journey.

Processes – collections can be arranged as part of a milk run around several sites or a bulk collection from a single site, to achieve a cost effective collection. For added security a dedicated journey direct from pick-up to processing site is also available. At extra cost, a "vehicle never unaccompanied" or a "non-stop" policy can be employed.

Tracked – upon collection, an asset register is taken and then confirmed with receipt at the processing site.

3.5 On-site Services

For some organisations, data security goes beyond protecting the company and its employees. It is fundamental to its operations, services and customers. In these circumstances allowing data to leave the site is not an option. Where security is paramount, a range of on-site solutions can be obtained to ensure that the business' critical data is completely secure.

3.5.1 On-site Data Capture and Auditing of Assets

The first step in any data security consideration is to understand exactly what the organisation's responsibility comprises of. It is possible to compile a comprehensive list of electronic assets at the organisation to ascertain what hardware and software is being disposed of. This allows the organisation to

appropriately sign off equipment from the asset register, whilst giving the IT manager information on software licenses available for reallocation or deletion. Working with the consultant, it allows the organisation to discern the most appropriate retirement strategy.

3.5.2 On-site Data Erasure

Specialist rigs can be brought to the organisation's site. Using these rigs, an operator is able to securely destroy the data on up to 1,000 hard drives a day. The system would use a software deletion package such as Blancco Data Cleaner and so is approved to HMG IA Standard No. 5.

Blancco Data Cleaner is also available to be deployed through a remote connection. Using this technology combined with the coverage offered by a company such as Sims Lifecycle Services, means that on-site data deletion can occur at any remote location around the world. Effectively preparing the device for local recycling or unsecured logistics to your nearest provider.

3.5.3 On-site Degaussing

Portable degaussing units are available to operate an on-site data sanitisation process.

3.5.4 On-site Physical Destruction

Dedicated services now exist that are able to transport a hardware destruction process capable of meeting Government recognised secure destruction standards. A truck able to power the appropriate shredder technology is able to reduce a range of media down to less than 6mm or 2mm flakes.

This allows the organisation to witness the destruction of a range of data bearing items such as Hard Drives, USB Sticks, CD ROMs, etc.

For smaller budgets, or remote locations, Hard Drive crushers are also available. These highly portable devices are able to break a hard drive and shatter its sensitive platters. Although not rendering the hard drive highly secure, it will make recovering data very difficult, allowing relatively safe transport to a secure destruction facility.

3.5.5 Data Centre Decommissioning

A combination of the above services provides the capability for the complete and secure decommissioning of large storage arrays or of complete data centres. Full reporting would be available on the decommissioning process, from data and hardware destruction to an inventory of all materials removed from site.

Audited sub-contractors can offer specialist services such as decommissioning and removing bulky equipment from difficult locations such as air conditioning banks from roof-tops.

4.0 The Recycling Process for IT and other Electronics

All IT recycling processes operate, at a fundamental level, in a similar way. The first stage of the process is to break the electronic products down into small flakes, around the size of a corn-flake, or smaller where data protection requires. This naturally liberates materials away from each other. The operation will then employ a series of processes to achieve the separation and refinement of the downstream materials.

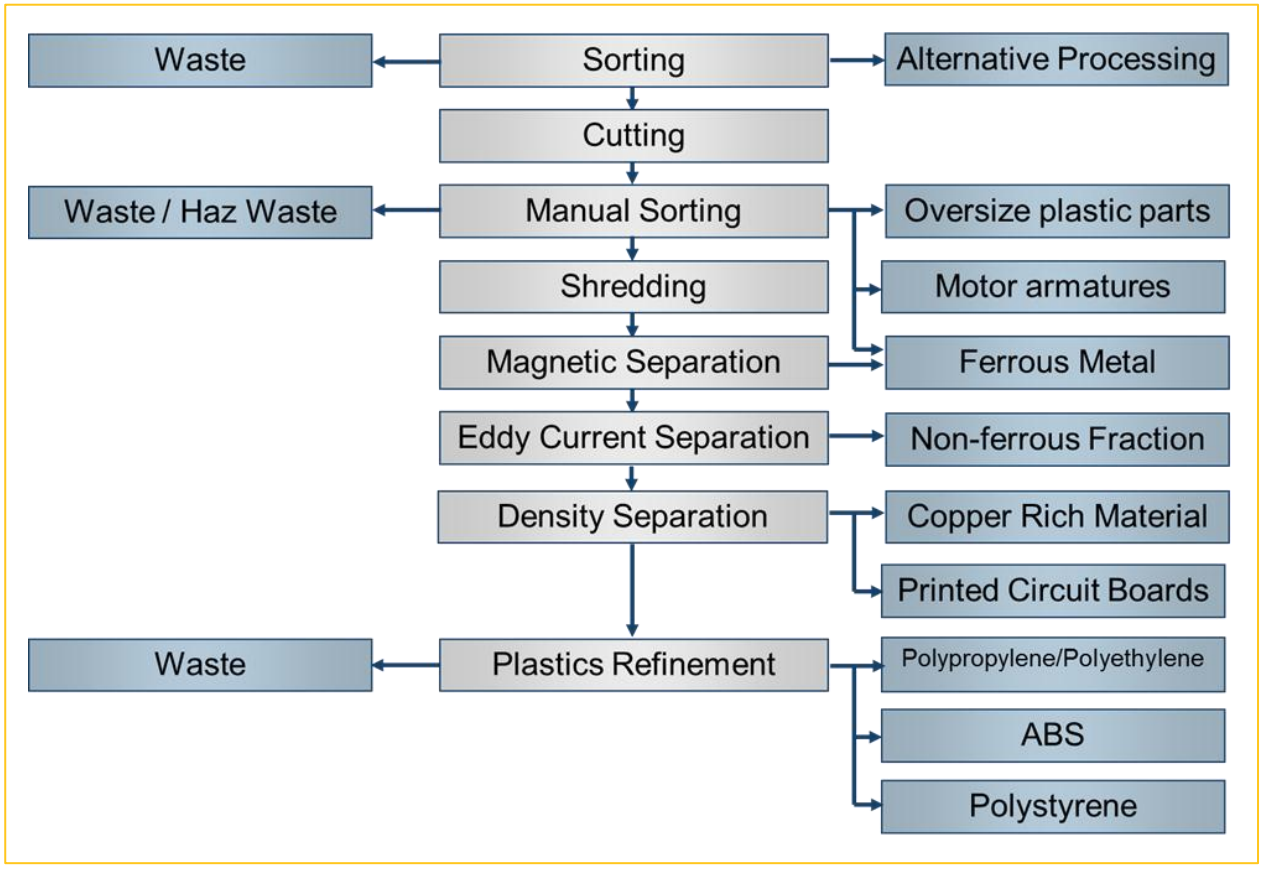

Fig. 5. The electronic waste recycling process

Figure 5 demonstrates the core IT waste recycling process in the silver boxes down the centre. The left-hand-side demonstrates waste outputs which will go for recycling, further treatment or appropriate environmentally compliant disposal. The right-hand-side demonstrates recyclable material outputs which go for further refinement or sale into the global commodity markets.

Sorting – this initial stage is done at receipt of goods. It might include recognising products that are not suitable for the process (LCD monitors, which contain Mercury vapour back-lamps) or other materials such as pallets and pallet wrap which will be separated from the process material.

Cutting – a pre-process which simply breaks the products up into very large pieces, allowing manual sorting to identify and remove certain items and materials.

Manual Sorting - Oversize plastic will be removed here, as early segregation allows for cheaper processing of the materials. Armatures out of electric motors are removed as their magnetic properties will confuse the later separation processes. These are heavily copper rich and can be sold as a commodity. Large pieces of metal which might damage the later processes are also removed at this stage. Finally hazardous waste such as batteries are identified and removed.

Shredding – the main process for size reduction of products into "cornflake" size pieces. This liberates materials from each other, ready for sortation. By altering the "grid" size of this stage, the size reduction can be reduced to less than 6mm, which ensures data security to Government standards. Normally a larger grid is used as it makes shredding and downstream separation processes more efficient.

Magnetic Separation – high powered magnets remove the ferrous metals such as iron and steel.

Eddy Current Separation – a rapidly alternating magnetic field creates "eddy currents" which effect non-ferrous metals, forcing them to leap away from the conveyor, allowing separation from non-metallic materials. Non-ferrous metals can be sold as is, however in the UK, Sims Recycling Solutions also operates a Dense Media plant which is able to further refine these metals into separated aluminium, copper, etc.

Density Separation – The next process is concerned with precious metal refining. It targets the separation of copper wire and printed circuit boards from non-metallic materials such as glass and plastic. The wire and can be sold to smelters for precious metals recovery. Sims operate advanced refinement processes that are able to refine circuit boards into grades that enhance smelter recovery.

Plastics Refinement – Sims Recycling Solutions have developed a plastics refinement process that is able to refine mixed plastics into saleable commodities for low grade use. Research and Development is currently implementing technology to refine certain polymers, such as ABS, to quality levels that can be re-used in high grade applications.

5.0 Relevant Legislation

There are a number of Directives and Legislation concerned with the reuse and recycling of Electronic Equipment:

RoHS Directive (Restriction of Hazardous Substances) – Electronic Equipment must be manufactured without certain identified hazardous materials.

Energy using Products Directive – a directive driving the Eco-friendly design of electronic equipment ensuring they have smaller carbon footprints in their design, manufacture and use.

Batteries Directive – ensuring batteries are being recycled and use of hazardous materials in future batteries are controlled/reduced.

WEEE Directive – concerned with making the producers (manufacturers/distributors) of electronic equipment responsible for the appropriate recycling of that equipment, at the end of its life. Part of the WEEE directive is IPR (Individual Producer Responsibility), a future development encouraging producers to achieve cost savings and other benefits through designing easier to recycle products.

Hazardous Waste Regulations – a UK specific legislation that dITates, amongst other things, how electronic waste must be recovered, processed and transported.

Trans-Frontier Shipment Regulations (TFS) – regulations that govern the shipment of "waste" to and from the UK to and from other countries.

The majority of this legislation effects producers of electronic equipment as opposed to end users. However they are relevant to end users in the following cases:

- The WEEE Directive is relevant to a business if they are disposing of equipment older than August 2005, if they are not replacing the equipment on a like for like basis
- If the business end-user decides to take personal responsibility for the disposal of equipment and they do not deem it as re-usable, they need to comply with the WEEE directive
- Any materials an organisation must dispose of, will be affected by the Hazardous Waste Regulations
- Any equipment being disposed of, the producer (manufacturer/owner) has a duty of care to ensure that it is being disposed of in a legislatively compliant manner

5.1 The IT Asset Disposal Marketplace

This new legislation has helped to create an innovative industry in the form of Electronic Asset Recovery and Recycling. This industry consists of a number of different types of organisation: charities, SMEs and large professional businesses. All of which can offer the client varying levels of service that, importantly, will comply with legislation.

Unfortunately a fourth player operates in the market, opportunists. These "businesses" exist to make money and are happy to flaunt law and best environmental practice to do so. Common practice is to simply dump waste illegally in the UK or more commonly transport it illegally overseas, exposing your company to a range of data security, environmental and brand protection issues.

When shipped overseas it often ends up in third world countries that simply do not have the infrastructure to treat this waste appropriately. The practices used to recover value are extremely harmful to the environment and directly to the people handling the waste.

It is vitally important to question your supplier to ensure they are operating compliantly.

Certain Standards and Certifications are now available. Some of the main ones are listed below:

ADISA Accredited – Asset Disposal and Information Security Alliance. A professional body pushing for recognised standards in the UK, EU, America and Australia.

NAID – National Association for Information Destruction, the International Trade Association for Companies Providing Information Destruction Services in the US, Australia, New Zealand, Europe and Canada.

PAS141 – a UK standard detailing a recognised process for demonstrating appropriate testing of equipment to certify it is ready for reuse.

R2 (Responsible Recyclers) – This is an American standard detailing appropriate measures to ensure the responsible recycling of electronic waste. It is currently gaining ground globally. The standard was developed by the American Environment Protection Agency with industry stakeholder including Leading Electronics Manufacturers.

eStewards – Another America standard detailing appropriate measures to ensure the responsible recycling of electronic waste. Again, attempting to gain ground, globally, this standard was developed by BAN (Basel Action Network) an organization focused on confronting the global environmental injustice and economic inefficiency of toxic trade (toxic wastes, products and technologies) and its devastating impacts.

WEEELABEX – European standard detailing appropriate measures to ensure the responsible recycling of electronic waste. This standard has been developed by the WEEE Forum – the industry group for European WEEE Compliance Schemes.

5.2 Important Questions to Ask your Service Provider

As a producer of surplus electronic assets for re-use, a business has a duty of care to protect their customer's and employee's data. As a producer of electronic and/or hazardous waste, an organisation has a duty of care to ensure it is handled and processed appropriately. It is important to find the best priced service, but also to ensure you are getting the appropriate service levels that comply with legislation and do not expose your organisation to risk:

Can the provider demonstrate the assurance of Data Security?

If the asset recovery company is only talking about hard drives from computers and servers they are NOT appropriately looking after the organisation's assets. Data security exposures exist in the hard drives and flash cards routinely contained in printers, scanners, faxes, cell phones, Blackberries and other communication devices. It also exists in network equipment containing network-specific information such as static IP addresses. Ask to see their security credentials, i.e. what standards they operate to.

Can the provider demonstrate evidence of their ability to transport, store and manage waste?

Recycling electronics requires various permits in relation to the transport, handling, storage and management of waste. Operators should be registered with the Environment Agency (EA) or Scottish

Environment Protection Agency (SEPA). They should be able to produce relevant licenses for their operations. Evidence of other recognised management systems such as ISO9001 Quality Systems or ISO14001 Environment Management systems will give added reassurance. Are they able to provide copies of their Environmental, Health, and Safety policies and practices including emergency response plans, employee training plans and records?

Can the provider show how they re-furbish and recycle responsibly?

The service provider needs to manage the organisation's environmental exposure both at the arising of assets and at the final disposition of the assets or their recovered materials. Is the provider able to demonstrate to whom they have re-sold the electronic assets and in what state those asset were. Can the provider demonstrate responsible downstream processing; especially for Hazardous Materials such as batteries, Cathode Ray Tube glass, mercury bulbs, PCB capacitors and so on. Do they have copies of paperwork that the organisation can review detailing the final customers?

What locations and equipment does the provider have?

Processing high volumes of electronic assets requires significant investment. Talk to the provider and try to understand if their capabilities match their words:

Asset Recovery is mainly a manual process; a highly efficient business with 150 employees can cater for around a million units per year. See Figure 6, part of Sims Lifecycle's Dumfries processing line.

Meanwhile a compliant recycling line will require a large capital expenditure and will see bulky equipment housed in a good sized facility. See Figure 7, a plant capable of recycling over 100,000 tonnes per year.

Fig 6. Gravity feed conveyors and Sims Lifecycle Services' Asset Recovery operation

Fig. 7. Sims Recycling Solutions WEEE Plant, Newport

Have you visited and audited their operation?

Most important, for an organisation choosing a recovery and recycling partner, is to visit the provider's site. It is important to gain an understanding of their processes and to take time to ensure appropriate licenses and audit trails are in place to ensure the organisation's duty of care is being met.

6.0 Who are Sims Lifecycle Services?

Sims Lifecycle Services was created 7 years ago and has since acquired the expertise and operations of several other specialist companies, globally. The service enables businesses and public sector organisations to sustain the value of IT and electronic equipment, in a legally compliant, data secure, fully traceable and environmentally sustainable manner.

Sims Recycling Solutions has been operating in the recovery and recycling of electronic equipment for over 15 years. It is the world's leading electronics recycler with 50 sites across 5 continents operating a dedicated research and development team to ensure the evolution of class leading services and recovery and recycling operations.

Sims Lifecycle Services and Sims Recycling Solutions operate as dedicated business disciplines to ensure the relevant expertise and dedication of service development is supported and enhanced. Our management systems then deliver coordination between these divisions which, in turn, provides a comprehensive chain of custody throughout the recovery and recycling process.

All of Sims' IT recovery and recycling operations are certified to ISO 9001 Quality Management Systems, ISO 14001 Environment Management Systems and the OHSAS 18001 Health and Safety System. Specifically, Sims Lifecycle Services also holds the ISO 27001 Security Standard and safecontractor award.

Sims Recycling Solutions is a business of Sims Metal Management Limited, the global leader in the secure and sustainable management of resources for industry, organisations and the public-at-large. The company has an annual turnover of $9 billion and has its ordinary shares listed on the Australian Stock Exchange (ASX CODE: SGM) and its ADRs listed on the NYSE (NYSE SYMBOL: SMS).

Sims Metal Management Limited was named as one of the top 100 most sustainable corporations for the last five years at the World Economic Forum in Davos, Switzerland.

7.0 CONTACTS AND DETAILS

For more information on any of the topics mentioned in this document, please do not hesitate to contact us at the details below:

Tel: +44 (0) 1789 720 431

Email: Info.uk@simsrecycling.com

Web: www.simslifecycle.co.uk

Address: Sims Lifecycle Services
Irongray Business Park
Lochside Industrial Estate
Dumfries
DG2 0NR
UK