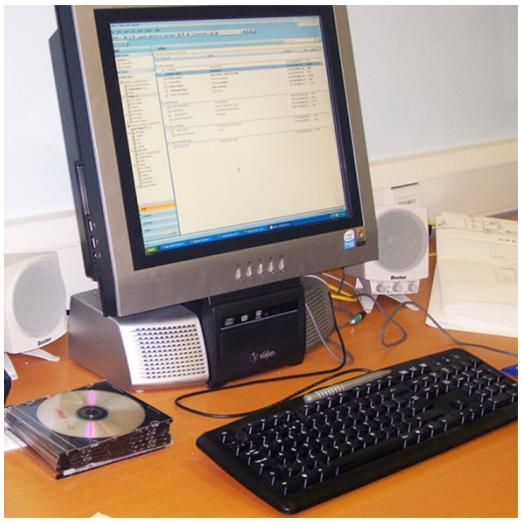
Computer Centre

Disposal of PCs and similar equipment, including destruction of data storage and licensed software



The purpose of this document is to explain procedures for disposal of PCs and similar equipment which have been used for University purposes, have been used to store University data, and/or have been loaded with an operating system and other software through University licensing agreements, in order to ensure the University's full compliance with its various contractual and legal requirements. The subject matter includes the destruction of data storage media and software licensed for use in furtherance of University activity.

October 2013

Document properties

Authority

Information Steering Group

Sponsor

Director, Computer Centre

Responsible officer

Assistant Director, Computer Centre (Governance and Corporate Services)

1 Overview

When a PC or similar device reaches the end of its useful life for the person to whom it was first issued by the University, there remains the issue of its disposal. The leasing contracts which are in force for significant quantities make disposal simple: the machines are not owned by the University, and return to the lessors at the end of the leasing period, when all data are destroyed as a part of the contract. The closing date is well known in advance, so there is ample opportunity for the orderly transfer of University data to secure storage well in advance of the removal day.

If the University has purchased the device, or has otherwise acquired title to it, there are ongoing legal, ethical and financial implications, and it is the responsibility of the member of staff who has been using the machine (the 'outgoing keeper') to discharge all responsibilities attendant upon the disposal of the PC. It is a clear dereliction of duty for any member of the University to ignore or seek to by-pass these responsibilities (including the responsibility to undertake a full economic costing of any action which deviates from the default). The simplest, cheapest, and most effective means of ensuring that data are not transferred to a new keeper is by the physical destruction of the hard drive: thereafter, the device is in a position to be re-used by a new keeper, or to be transferred for destruction through a waste management contract.

Some machines are provided by a research sponsor and remain the property of the sponsor, and there may be similar third-party ownership in other cases. Research data should be transferred in a legally compliant fashion to alternative storage, and destruction/replacement of the hard drive agreed with the owner. If there are compelling reasons why such a course of action is untenable, permission must be sought for waiver authority from the Director of the Computer Centre.

Any other form of transfer — for example, as a hand-me-down to a charity — involves the University in significant cost and effort which is almost certainly out of proportion to any transferred benefit or value.

This document contains an annex which deals with data storage and licensing implications on the cessation of the carrying out of University business on privately-owned PCs and similar devices (normally in the personal ownership of persons employed by, or otherwise associated with, the University), whether the device is or is not at end-of-life.

2 The hard drive

The hard drive is where are stored the zeroes and ones which coalesce to form the operating system, the software and drivers loaded upon the PC, and the data generated by the user or loaded from other sources. All of these are subject to responsible treatment by the keeper of a PC: in our case the ultimate 'keeper' is Brunel University, though the individual 'outgoing keeper' has primary day-to-day responsibility. There is a small class of machines which are in third-party ownership

It follows that on disposal of the machine, we must discharge our duties with respect to all of the above. The simplest and surest way to ensure that we do not fail in these duties is to destroy the hard drive (just unscrew and remove it, and send to the Computer Centre for assured destruction): any new owner may then substitute a fresh, clean hard drive for only £40 or so, and thus be certain that she/he had no worries about integrity of data. Simply deleting the files is no remedy: all that this does is to unhook the pointers to the information to make it difficult to find. Difficult, perhaps, but by no means impossible.

There are many software tools which will painstakingly undelete (based on the information still stored even after deletion), and we cannot leave a future keeper with the opportunity (or temptation) to apply such software to the task of recovering parts of the PC's history. Equally, there are software tools which claim to wipe all data from the drive, but there is still the nagging doubt, especially if there is no watertight certification. And that doubt would destroy any defence in court. It just isn't worth the risk.

3 Data, compliance and intellectual property

What do we mean by 'data'? Clearly, data collected for research will count, and that may be the first data type which would be considered as having personal, sensitive or otherwise valuable material — whether the data contain details of interviewees' sexual preferences (clearly personal and sensitive) or measurements from a sensor (which could have value to others). However, the whole class of 'office data' — mail, calendar data, wordprocessed documents, spreadsheets, and so on — contains a wealth of personal data, and of intellectual property which must not be left to be picked up by the next keeper. Pictures, downloads, and the more ephemeral (one might hope!) classes of data such as browsing history: all must be kept from the prying eyes and money-grabbing lust of a future keeper. Recent compliance penalties have been of the order of hundreds of thousands of pounds for acts similar to leaving Brunel data on a PC after disposal.

It is important to realise that even transfer within Brunel is not free from compliance responsibilities: data stored by one person is, on the whole, unlikely to be needed by another (the concept of 'purpose limitation' is strong in data protection legislation, and is getting stronger on legislative review), so on-site forays into PC hand-me-downs or scavenging are to be discouraged most strongly.

4 Software and licensing

Software is licensed by the developers/vendors, and each product has different licensing restrictions. Any software which allows transfer of title will seek the name of the title-holder on loading, so the original media (or the requisite keys to access the software online) may be conveyed to a new keeper: there is no need to retain the software on the machine, and again the integrity of the new keeper's holdings is assured by a fresh loading. In the case of a machine owned by a third party, the same will apply: at the end of Brunel use of the machine, data will be transferred to other storage media (maintaining, of course, due regard for all compliance responsibilities) and software re-loading will be made possible by the

conveyance of the original media, thus allowing the replacement of the hard disk for use by the next keeper and the destruction of the disk used for Brunel business.

Most software is restricted to Brunel use, and therefore must not be made available for use by another at the time of disposal. The penalties to the University are severe: in addition to financial redress sought by holders of copyright and intellectual property, the University could be excluded from educational discounts (often 90%), and of course would have a damaged reputation due to adverse publicity.

5 Operating system

If there is a valid OEM (original equipment manufacturer) licence for the operating system, there will be discs to re-apply that system, or at least, there will be a key/password with which to access a downloadable version). Many Brunel PCs have an operating system which is licensed specifically for Brunel use, so naturally that system must be removed before disposal to another keeper: if there is a legacy OEM licence, that may be applied by the new keeper, or a new operating system (probably one more in keeping with the times) may be purchased by the new keeper. The same will apply to machines in third party ownership: the system may be re-applied on a fresh hard drive, allowing for the destruction of the Brunel-era hard disk.

6 Leasing contracts

Like many other organisations and companies, Brunel has leasing contracts for many of its PCs and similar equipment. Decisions on whether to lease or buy equipment are governed by several factors: the 'cost of money' causes fluctuation in the monthly/quarterly leasing payments, there may be financial rules which debar certain transactions from the leasing option, and there are the more emotional ties to tangible 'ownership' which can often cloud the issue. Our leasing contracts have specific clauses which passes the responsibility for data erasure to the leasing company at end of lease: in this way, we are able to receive newly-leased PCs and to return same complete with hard drives (and mice/keyboards). A purchase leaves us responsible for disposal costs, which can be non-trivial (there are per-machine and generic costs), plus staff time to make each individual PC fit for disposal.

7 Costs

What costs are involved in destroying data on a hard drive? For a software solution which might get close to wiping everything 'beyond reasonable doubt', about £17 per drive — almost half the cost of a fresh drive on its own. But this isn't 'fire-and-forget': in order to brace ourselves for any questions about data remaining afterwards, we need to maintain an audit trail of the process of destruction, and that takes storage, software and (most importantly and expensively) someone's time. Simply watching over the data destruction takes staff time to interact with the process (which may take several hours for each drive): staff need to be trained how to do this, and we need to maintain awareness of the viability of the machines, of their components, and of their operating systems.

By contrast, physical destruction of the drives needs only a simpler audit trail of that destruction, the disposal of the unusable drives (just unscrew and remove, and send to the Computer Centre for assured destruction), and minimal staff intervention (or a contract which provides us with the first of these elements, and handles the other two).

8 Recycling and re-use

A driveless PC is re-usable (all other components being up to standard): all it needs is a fresh drive. By ensuring that this has to be provided by a new keeper (potentially, by a new keeper within Brunel), all minds are set at rest that the University has discharged its duties with respect to the PC regarding data, licences, WEEE regulations, and all the attendant requirements. Of course, the regulatory burden on the University is eased to the greatest extent through a properly constructed leasing contract.

There will always be seductive siren calls for 'donation for re-use', whether that is for staff family use (remember, no other family member should ever use a Brunel-registered machine, whether desktop, laptop or other device, since that breaks numerous legal conditions of use), for schools, or for staff members' pet charities — perhaps even their pet pet charities. But when we go beyond the doe-eyed glow of 'feeling nice', we need to come to reality. And the reality is that there are, in virtually every case, too many risks, too great a chance that we would be handing over a poisoned chalice, and too much cost (to be borne, usually, by units of the University other than that of the donor-decider) leaching away to provide insufficient real benefit. Many of these recipients — particularly in charity or volunteering roles — are undoubtedly well-meaning, but amateur, and they are vulnerable to being sucked into technology and issues that they can neither understand nor manage effectively. That raises the spectre of a dependency culture upon the donor, and our technical staff simply do not have the time to devote to non-primary duties. The most effective way to help a charity keep pace with technological needs, from a corporate and personal point of view, remains the simplest — to write a cheque.

There is another, more sinister side to this, in that there are some set-ups which purport to be either charities or recycling factors, but which are in effect criminal dealers in the data and identities which can be gleaned from insufficiently purged devices. It's true of PCs, and it's true of mobile devices such as phones or tablets. We simply cannot take such a glaring risk to the University's reputation, and the effort in undertaking due diligence with respect to such operators far outweighs any benefit.

A machine in third-party ownership should be returned with a fresh hard disk, unless the owner indicates that the return will constitute the end of the machine's life, in which case the machine will be returned in a driveless state. Any variation from this will require an explicit waiver from the Director of the Computer Centre, who must be content that no University data will be leaked. All costs of such a variation will be met by the outgoing keeper.

9 Conclusion

Where there are many conditions and responsibilities competing for attention, simplicity transcends being a virtue and becomes a necessity. Financial rectitude and simple human respect for other warrant-holders demands that we do not spend money unnecessarily, and that we do not spend others' money without agreement. We must do all we can at all times to avoid legal/ethical vulnerability, and to identify and account for the full economic cost of actions (cross-charging to the cost-centre of primary responsibility as appropriate).

The simplicity and finality of leasing contracts (with appropriately strong disposal clauses) makes this an ideal default where financial regulations allow. The more pervasive these contracts are, the easier and more efficient the asset management will be. The secondary benefits which accrue (such as the lifecycle refreshment's avoidance of 'operating-system drag') simply underline the benefits of this *modus operandi*.

Where leasing is ruled out by financial regulations, or for other reasons (which have been star-chamber stress-tested), disposal of a PC should incorporate the destruction of the hard drive, with the removal logged as part of the data audit trail. The hard drive must be removed and sent to the Computer Centre before committing the rest of the PC to Waste Management: any labour costs other than the Computer Centre's destruction service will be borne by the outgoing keeper's cost centre. In the unlikely event that it is impossible to dispose of a PC without destroying the hard drive, the data purging must be carried out by a competent technician, with the full cost (including licences and labour) being charged to the outgoing keeper's cost centre.

It is vitally important that everyone involved in the disposal of PCs is fully cognisant of, and up to date with, all relevant regulatory mechanisms, including (but not limited to) areas such as data protection, hazardous/electronic waste, audit and financial concerns, and identity integrity, and that such status is assured through appropriate logs and documentation.

Protocol for the disposal of PCs and similar equipment, and destruction of data and/or licensed software: machines owned by Brunel University

1 In order to comply with legal and moral requirements, it is important that the University disposes of PCs and similar equipment according to relevant legislative and ethical standards. In particular, we must ensure that no University data or licensed software (including any specially-licensed operating system) may be transferred to a subsequent keeper of the PC.

2 A rigorous audit trail of disposal will be kept by outgoing keepers of PCs and similar equipment. This will note the date and destination of disposal, along with the serial number and description of the PC. The Brunel University Equipment Disposal Form is to be used, and all Financial Procedures apply. If the PC is not leased, the audit trail will also note the serial number and description of the hard drive, and the date of its removal from the PC by the outgoing keeper and its delivery to the Computer Centre for destruction, using a separate Brunel University Equipment Disposal Form in respect ofthe hard disk. *Through this audit trail, the University will be assured that there is no breach of licensing regulations, of data privacy laws, of waste management regulations, and of any other relevant legal instrument through any re-use of the hard drive by a subsequent keeper.*

3 The keeping department or similar unit of the University will maintain an audit trail of each PC in its care, noting each successive physical location of the PC and its eventual disposal. *Through this process, the University will always have a complete historical record of the PC's deployment while in University hands.*

4 It is the responsibility of the outgoing keeper of a PC or similar piece of equipment to remove any hard drive from a PC which is owned by the University, save with an explicit waiver issued by the Director of the Computer Centre. In particular, the outgoing keeper must take notice that any work undertaken by anyone else to destroy all data on the hard drive will be charged at full economic cost to the outgoing keeper's cost centre. *In this manner, the University will be assured of the efficiency and effectiveness of the disposal procedure for hard drives and their data.*

5 The Computer Centre will accept all removed hard drives for assured destruction. Save with the explicit authority of the Director of the Computer Centre, no hard drive removed from a University-owned PC may be destroyed by any other party. *Through this procedure, the University is assured of the destruction of all de-serviced hard drives in compliance with relevant legal and ethical standards.*

6 The University's Waste Management Unit is responsible for the disposal of all other parts of de-serviced PCs (with the exception of those PCs returned to lessors under a leasing contract). *In this way, the University is assured of the disposal of all de-serviced PCs in compliance with relevant legal and ethical standards.*

Protocol for the disposal of PCs and similar equipment, and destruction of data and/or licensed software: machines leased by Brunel University

1 In order to comply with legal and moral requirements, it is important that the University disposes of PCs and similar equipment according to relevant legislative and ethical standards. In particular, we must ensure that no University data or licensed software (including any specially-licensed operating system) may be transferred to a subsequent keeper of the PC.

2 A rigorous audit trail of disposal will be kept by outgoing keepers of PCs and similar equipment. This will note the date and destination of disposal, along with the serial number and description of the PC. *Through this audit trail, the University will be assured that there is no breach of licensing regulations, of data privacy laws, of waste management regulations, and of any other relevant legal instrument through any re-use of the hard drive by a subsequent keeper.*

3 The keeping department or similar unit of the University will maintain an audit trail of each PC in its care, noting each successive physical location of the PC and its eventual disposal. *Through this process, the University will always have a complete historical record of the PC's deployment while in University hands.*

4 Any leasing contract for the supply of PCs and similar devices must contain a clause which charges the lessor with the assured destruction of data on hard drives. In the case that further measures must be taken (for example, at the behest of a research sponsor), the outgoing keeper must take notice that any work undertaken to destroy all data on the hard drive prior to return to the lessor will be charged at full economic cost to the outgoing keeper's cost centre. *In this manner, the University will be assured of the efficiency and effectiveness of the disposal procedure for hard drives and their data.*

5 The Computer Centre will, under any waiver from 'destruction by lessor' (which waiver must be obtained from the Director of the Computer Centre in advance of end-of-lease) accept all removed hard drives for assured destruction. Save with the explicit authority of the Director of the Computer Centre, no hard drive removed from a University-leased PC may be destroyed by any other party. *Through this procedure, the University is assured of the destruction of all de-serviced hard drives in compliance with relevant legal and ethical standards.*

6 The University's Waste Management Unit is responsible for the disposal of all other parts of de-serviced PCs (with the exception of those PCs returned to lessors under a leasing contract). *In this way, the University is assured of the disposal of all de-serviced PCs in compliance with relevant legal and ethical standards.*

Protocol for the disposal of PCs and similar equipment, and destruction of data and/or licensed software: non-leased machines in third-party ownership

1 In order to comply with legal and moral requirements, it is important that the University disposes of PCs and similar equipment according to relevant legislative and ethical standards. In particular, we must ensure that no University data or licensed software (including any specially-licensed operating system) may be transferred to a subsequent keeper of the PC.

2 A rigorous audit trail of disposal will be kept by outgoing keepers of PCs and similar equipment. This will note the date and destination of disposal, along with the serial number and description of the PC. The audit trail will also note the serial number and description of the hard drive, and the date of its removal from the PC by the outgoing keeper and its delivery to the Computer Centre for destruction. Details of any replacement hard disk will also form part of the audit trail. *Through this audit trail, the University will be assured that there is no breach of licensing regulations, of data privacy laws, of waste management regulations, and of any other relevant legal instrument through any re-use of the hard drive by a subsequent keeper.*

3 The keeping department or similar unit of the University will maintain an audit trail of each PC in its care, noting each successive physical location of the PC and its eventual disposal. *Through this process, the University will always have a complete historical record of the PC's deployment while in University hands.*

4 It is the responsibility of the outgoing keeper of a PC or similar piece of equipment to remove any hard drive from a PC which is not subject to a leasing contract as described above, save with an explicit waiver issued by the Director of the Computer Centre. In particular, the outgoing keeper must take notice that any work undertaken by anyone else to destroy all data on the hard drive (save under the standard leasing contract) will be charged at full economic cost to the outgoing keeper's cost centre. *In this manner, the University will be assured of the efficiency and effectiveness of the disposal procedure for hard drives and their data.*

5 The Computer Centre will accept all removed hard drives for assured destruction. Save with the explicit authority of the Director of the Computer Centre, no hard drive removed from a PC in third-party ownership for the purpose of destroying University data and/or licensed software may be destroyed by any other party. *Through this procedure, the University is assured of the destruction of all de-serviced hard drives in compliance with relevant legal and ethical standards.*

6 The University's Waste Management Unit is responsible for the disposal of all other parts of de-serviced PCs (with the exception of those PCs returned to third-party owners). *In this way, the University is assured of the disposal of all de-serviced PCs in compliance with relevant legal and ethical standards.*

Annex

Management of University data and licences on private machines

Definition

For the purposes of this document, a *private machine* is a device which is not corporately owned or leased by the University, nor is owned by a third party such as a research sponsor or contracted company. In many cases, a private machine will be owned by a member or associate of the University: it is the use of such a machine for occasional University business (typically when the owner is away from the workplace) which is addressed here.

Overview

We know that people use private machines for Brunel business: this should just be for occasional use. In the case ofa staff member, if there is a need for regular off-campus use, then a case may be made for an appropriate machine to be provided by the local department (or similar cost-centre unit). The standard procedures and protocol may be followed, and the staff member is able to segregate Brunel use from personal use, and to be the sole user of the provided machine.[1]

However, even the checking of electronic mail may leave Brunel data on a machine (a downloaded attachment, say, or a journal history). It follows that, when the machine is no longer 'kept' by the Brunel member (say, by its being given to a family member leaving for university), a rigorous destruction of data must take place. Ideally, this would involve the replacement of the hard disk as per a Brunel-owned machine.

Maintenance of security during period of use

During the period of Brunel use, the machine must abide by the conditions of maintaining up-to-date and operative anti-virus and similar protections. It must not be left on unattended, where others may gain access to stored Brunel data, and should be password-protected with standard password security features (strong password never written down, password changed at any potential compromise, etc.).

If the machine is lost or stolen, the incident should be reported immediately to the University's Information Access Officer as a potential data leakage, and all reasonable steps must be taken to retrieve the machine or to secure the data's inaccessibility, including immediate change of network password (and any associated passwords) and remote freezing of the machine if at all possible.

---

[1] Users are reminded that a machine provided by the University must not be used by any other person (*e.g.*, a family member): this is to maintain the integrity of any Brunel data/access

Data/licence destruction at end of use

If Brunel-licensed software has been loaded on the machine, it must be removed beyond retrieval when Brunel use ceases (including the handing on to a family member). Likewise, Brunel data must be removed beyond retrieval. If at all possible, this should be effected by replacing the hard disk and conveying the old disk to the Computer Centre for assured destruction. This will allow for the reloading of the licensed operating system and any software licensed privately (rather than as a Brunel licence).