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

Document properties

Authority

Information Steering Group

Sponsor

Director, Computer Centre

Responsible officer

Assistant Director, Computer Centre (Governance and Corporate Services)

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, dataee eTJ0m 21(e)-2smatae-isme-iee1oe[-o, I0C s2-iin1 am0.003pe(e)-m-6(e)(e(0.)TJ-6(t)-6(tar)-

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

9 Conclusion

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

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.

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

Annex

Management of University data and licences on private machines

Definition

For the purposes of this document, a 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 (, 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).