

Software Management Checklist

This publication is aimed at UK further and higher education staff working in areas related to knowledge transfer, work based learning, community links, outreach, CPD, employer engagement, wider participation, and lifelong learning.

It is one of a series of publications produced by JISC Legal to raise awareness of the potential legal issues related to the use of technology by colleges and universities in relation to their business and community engagement activities.

Please note: this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

12 July 2007

If you have Adobe Acrobat Reader installed on your computer, you may download a PDF version here - <http://www.jisclegal.ac.uk/pdfs/BCESoftwarecheck.pdf>. (Recommended for printing.) Acrobat Reader is available free from Adobe's web site - <http://www.adobe.com/>.

Table of Contents

1.	Introduction	1
2.	Know what software you have	1
3.	Know what licences you have	2
4.	Maintain a software register	2
5.	Have a software policy	2
6.	Conduct regular audits	3

1. Introduction

This checklist is designed to assist colleges and universities manage the software which they licence from third parties.

2. Know what software you have

- identify the machines (desktop PCs, laptops and servers) which you have; and
- check and note the software on each machine (i.e. the application, version and any upgrades).

You should be able to trace when and from whom the software was acquired and tie this to the relevant invoice. You should also be able to confirm if the software was

purchased in CD Rom format, downloaded or OEM installed.

You should also identify any copies which have been made of the software, together with the reason for such copies (i.e. for legitimate back purposes).

3. Know what licences you have

- identify the number and type of licences which you hold; and
- compare this against the software which you have.

You should assess what licences you have (both number and type), and what those licences allow you to do.

For instance, you may be using software without any licence at all. Alternatively, the number of users may exceed that permitted by the licence, or the activity being performed may fall out with the scope of permitted use (i.e. software subject to an academic licence being used for commercial activities).

Where licence coverage is insufficient, additional or replacement licences should be purchased.

4. Maintain a software register

- establish a centralised register of your software and licence coverage;
- centralise and standardise software purchasing;
- have clear guidelines on the maintenance of the register.

All software and licences held should be recorded on a centralised software register. When the register has been created, it is essential that it is kept up to date. It should, at any given time, give an accurate report on the software which you hold, the number of licences and any restrictions on use.

Ideally, the purchasing (and/or retirement) of software should be centralised – this will assist in ensuring that the software register is kept up to date. If this is not practical, there should be a clear procedure for any and all purchases (or retirements) to be reported to the maintainer of the register as soon as possible.

All documentation pertaining to the software (i.e. licences, invoices, user manuals, accompanying documentation) and any media (i.e. CD ROMs) should be retained and filed in a secure, centralised location in case it is ever needed to verify entitlement.

There should also be a standardised procurement procedure – be clear who you can purchase software from and what you expect to receive in return.

5. Have a software policy

- use of unauthorised or illegal software is a risk

There are a number of risks. You could be sued for copyright infringement if you use software without a licence and could be the subject of adverse publicity. Illegal or counterfeit software also exposes your system to risk (for instance, viruses).

A software policy will help to mitigate these risks by letting employees and students know what uses are acceptable and what uses are not. This policy must be implemented and, where appropriate, enforced.

6. Conduct regular audits

- implement an audit strategy

You should conduct a software audit at regular intervals (i.e. once a year) to ensure that you are and continue to be fully licensed. If you have maintained a software asset register, this will involve checking that the register is complete and up to date.

You should consider your software licences in the context of your operational requirements. Have you expanded your activities? Have you ceased providing a particular course or activity? These matters will impact upon your software requirements.

If any inaccuracies are identified, you should assess how this occurred and take appropriate remedial action.

John Reid

JISC Legal

12 July 2007