Financial Control no10
Security of equipment, assets and financial system

Index:

Updates Sept 2023: none

1. Introduction

The school's equipment and assets should be properly recorded and safeguarded against loss. Asset Register information, available from Schools Financial Services, contains guidance on the maintenance of asset registers and the general safeguarding of school assets and equipment. The asset register can be completed using SIMS FMS6, other computerised system or manually.

Efficiency and security is necessary for any computer system being used for the financial management of the school.

2. Key Controls and Procedures for assets

2.1 Upon receipt, all items of value over £200, or of a lower value if of an attractive nature, should be recorded in an asset register. The register should include details such as make, model and serial number for identification purposes. The item should also be visibly security marked.

2.2 The asset register should be held securely. Preferably off site so that it is available to support an insurance claim in the event of any loss resulting from fire, flood, theft, etc. (Schools should ensure electronic records are included in the off-site backup procedure through Cantium (EIS) or their designated provider.)

2.3 The school must also adopt a basic authorisation procedure for the disposal of assets, usually included in the finance policy. Items of value that have been declared as obsolete for school use should be properly written-off and disposed of securely and/or to the benefit of the school.

2.4 Agreement for such write offs should be made by the full governing body or sub-committee if delegated and such agreement is to be minuted within the appropriate meeting minutes.

2.5 Items of value should be stored in a secure place when not in use, e.g. in a part of the school protected by a security alarm system, or in lockable rooms or cupboards. If this is not possible items should be stored away from windows so that they cannot be seen from outside.

2.6 Any item borrowed by pupils or staff should be authorised by a designated officer, recorded and signed for in a loans book before it is removed from the school premises. The date the item is due to be returned, should also be recorded and, when it is returned, it should be checked into school and signed back in the book by the authorising officer.

2.7 The record should be kept up-to-date and entries monitored to ensure that the whereabouts of all equipment and assets are known at all times. Details include date, full details, name of the borrower, signature of authorising officer and date of return. Any loaned equipment should be returned to the school for the annual asset check to confirm its existence and condition.

2.8 In secondary schools, a designated officer should have the overall responsibility for monitoring the accuracy of records and the safeguarding of equipment/assets.
An annual stock take should be carried out and the results documented in the asset register. The register should be certified by the Headteacher, or designated deputy, each year to confirm its accuracy and that the check has been properly carried out.

{Back to top}

3. Key Controls and Procedures for finance system

3.1 Users should be allocated access levels according to their operational needs. User ID's and personal passwords should be kept secret and frequently changed to maintain security at least on a termly basis. An emergency list of authorised user ID's and passwords should be held securely to prevent unauthorised access. More than one person should be proficient in the operation of a system to ensure continuity in the event of the departure or long-term absence of the main system operator.

3.2 Back-ups of the system and data should be taken daily and should be stored in a secure place away from the server and in a fire-proof cabinet or safe. The data can be backed up remotely and stored with Cantium (EIS) or their designated provider. The records can then be reconstructed in the event of a major disaster.

3.3 All confidential information held on the computer system should be restricted and secure. Additionally, any output from the system that contains confidential and personal details should be subject to similar controls (The Data Protection Act which the school is required to register requires this).

3.4 Schools are required to maintain a current entry in the Data Protection Register with the ICO for a nominal annual fee.

3.5 The school should ensure that it complies with software copyright legislation, where software licenses are held for all the software installed at the school. Staff using computers should have signed a “code of conduct for software use” form.

3.6 There should be systems and procedures in place to prevent the introduction of viruses, including an E-safety policy.

{Back to top}