'Learn, Endeavour, Aspire, Respect, Nurture'

Oxspring Primary School
Head Teacher: Mrs S. Irwin
Co- Chair of Governors: Mr M. Cassidy / Mrs G. Mahoney

Revised: June 2021
Review date: June 2023

Information Assets Management Policy GDPR

BARNSLEY Metropolitan Borough Council

1. INTRODUCTION:

1.1.1 The Governing Body of Oxspring Primary School is responsible for the proper management and security of the school premises and the custody and physical control of all other assets including machinery, furniture, equipment, stock and other assets such as cash (HLT – Financial Procedures Manuals for Schools 7.1, April 2014 version).

1.2 THE ASSET REGISTER

1.2.1 Oxspring Primary School maintains an Asset Register of items held by the school that the Governing Body deems to be valuable and/or subject to an insurance claim. Moveable assets valued at £1000.00 or more must be recorded. Note that all Information Technology (IT) equipment must be recorded, regardless of their value.

1.2.2 The Asset Register should include the following information:

- Date of acquisition of asset
- Description of asset, including colour, a unique identification mark such as serial number and security marking, where appropriate
- For ICT/electrical equipment, a record of the model or other unique reference/security number
- Cost of the asset purchased
- Source of funding
- Location of the asset
- Details of the disposal of any assets, whether scrapped, sold or donated
- Details of the revaluation of an asset
- Items used by the school but owned by others (e.g. leased items) supported by a note of ownership

1.2.3 Where possible, the Asset Register should be held within the school's financial system, rather than as a hardcopy document.

1.2.4 A copy of the Asset Register must be kept in a safe, fireproof place, and be available for inspection.

1.2.5 Acquisitions and disposals should be recorded on the register at the time of acquisition or disposal and reported to the Governing Body.

1.2.6 The Governing Body must ensure that the Asset Register is kept-up-to-date and is reviewed at least once a year. The review must include the physical check of the assets and must be performed by someone other than the person maintaining the register. The Asset Register should be certified and dated on completion of the review.

1.2.7 The upkeep of the Asset Register can be particularly important for insurance reasons, as policies will often limit the insurance of equipment etc to those items present on the school asset register.

1.2.8 The Register should be reconciled annually with the School's Insurance Services records. Where the school participates in the Council's insurance programme, the register submitted to the Council should contain all audio/visual/ICT items

1.3 LOANING ASSETS

1.3.1 An asset can be loaned to staff of the school, and Oxspring Primary School must keep a log of such loans. Where a loan of asset could be deemed a benefit in kind and therefore have tax implications for the individual, the relevant paperwork must be completed.

1.4 DISPOSING OF ASSETS

1.4.1 The Governing Body of Oxspring Primary School may dispose of assets through sale, donation or scrapping.

1.4.2 Assets that have been disposed of must be removed from the Asset Register, and the insurer notified.

1.4.3 For every disposal, the Governing Body or the person who is maintaining the Asset Register must:

- Record the reasons for the disposal
- Be able to demonstrate that the assets are either obsolete or surplus to requirements

1.4.4 The Headteacher must appoint a single person (ICT technician) to be responsible for disposing of assets, and inform them in writing that they are ultimately accountable for doing so. The responsible person's name must be clearly identified in the school's disposal file.

1.4.5 Any disposal of a capital asset must be made in accordance with the school's policy on purchasing and disposal and, where the disposal involves land and/or buildings funded by the LA, the school must obtain formal advice and approval from BMBC,

1.4.6 Oxspring Primary School must ensure that they adhere to the latest WEEE (Waste Electrical and Electronic Equipment) Legislation, which sets out the requirements for disposing of electrical/electronic equipment, (see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/292632/bis-14-604-weee-regulations-2013-government-guidance-notes.pdf and also https://www.hse.gov.uk/waste/waste-electrical.htm). The legislation states that such assets cannot just be thrown away, must be disposed of properly, either by:

- Donation to a charity (for refurbishment and re-use) – e.g. Tools for Schools
- Disposal by a specialist organisation, who will take such items away and recycle them.

1.4.7 Before disposing of computer equipment school must ensure compliance with Data Protection Act 1984 by erasing all personal data from the hard disk. Note that merely deleting files may not physically remove the data, which could be restored using specialist products. School must also ensure that any software products for which licences are maintained in-house are removed from the equipment prior to disposal.

1.4.8 Any member of staff who determines that an asset is surplus to requirement, or who is involved in the disposal, should never attempt to purchase it or take it for personal gain. There should be a clear separation of duties and the Headteacher must approve all disposals.

1.4.9 Official receipts must be issued for income received for disposed assets. Monies must be received and properly accounted for by someone who has not been involved in the disposal.

1.4.10 The income received from the sale of any asset must be treated as income in the school's budget, unless it relates to the sale of certain assets (such as land and buildings owned by the LA) or to income from a Public/Private Partnership (PPP) or Private Finance Initiative (PFI), which are subject to a specific agreement.

1.5 OBSOLETE ASSETS

1.5.1 Assets are deemed obsolete if they have no resale value.

1.5.2 Oxspring Primary School may donate surplus, obsolete assets to the voluntary sector or scrap them.

1.6 SURPLUS ASSETS

1.6.1 Where the possible sale value for an item or group of items exceeds a predetermined threshold value, the school should seek to dispose of them by quotation, competitive tender or public auction, unless approved by the Governing Body to do otherwise.

1.6.2 The threshold value should be set by the Governing Body

1.7 RETENTION OF DISPOSAL DOCUMENTATION

1.7.1 All documentation relating to the disposal of the asset must be retained for a period of six years after the disposal.

1.7.2 The following types of document should be retained:

- The Governing Body or Headteacher's written record declaring the asset surplus, and instructions to the person appointed as responsible for the disposal
- The advertisement
- The offers made
- The receipt

1.8 SECURITY – GENERAL

1.8.1 The Governing Body is responsible for the security of the school's assets.

1.8.2 It is responsibility of all Budget Holders to ensure that a yearly stock check is carried out during the summer term. Any missing items must be reported to the Governing Body.

1.8.3 Appropriate arrangements must be in place for the security of all assets. Security measures could include the following:

- Secure equipment and other assets by means of physical and other security devices (e.g. locked in cupboards)
- Authority to access these secured assets should be clearly documented
- All items in the asset register should be permanently and visibly marked as the school's property
- Maintain a record of any model or other unique reference/security number in the asset register
- Clearly mark any portable equipment that is vulnerable to theft with the name of the school

1.8.4 Items which are easily portable and saleable (videos, televisions, computers, cameras, etc) must be security marked and kept securely locked away when not in use, particularly overnight. Keep a separate record (in the Asset Register) of any model or other number unique to your machines.

1.8.5 Items of school property should not be removed from the school premises without the appropriate delegated authority.

1.8.6 Should property be removed from the school premises, the school should:

- Establish the position related to insurance before the assets are taken off site
- Be aware that assets on loan for extended periods or to a single member of staff on a regular basis may be deemed a benefit-in-kind, which may be subject to taxation
- Keep a record of all assets removed from the school premises
- Update the record when the assets are returned

1.9 COMPUTER SECURITY AND PROTECTION

1.9.1 School computer systems hold sensitive financial and personal data. School must, therefore, take appropriate action to ensure that equipment and data is kept secure.

1.9.2 School should have a written ICT Security Policy, which should encompass the guidelines for protecting hardware and software, set out below.

1.10 PROTECTING HARDWARE

1.10.1 The main dangers to hardware are:

- Loss through theft
- Damage (accidental or otherwise)

1.10.2 To minimise the danger of loss or damage, the machines should be:

- Labelled with a unique asset number
- Entered onto the school's asset register with their serial numbers
- Correctly positioned (i.e. towers not laid on their sides)

1.10.3 If possible, the machines should also be:

- Not visible from outside the building or to the public generally
- Kept in a locked room when not in use, particularly overnight
- Where possible, secured to furniture
- Labelled, marked with indelible pen or have the name of the school soldered onto the case

1.10.4 To minimise damage and the chances of the machines being damaged all users should:

- Refrain from eating or drinking whilst working on the machines
- Never move or attempt to clean a machine without first obtaining the IT co-ordinator's advice
- Ensure any loose cabling into the machine is not in danger of being stood on or tripped over by staff
- Know who to contact in the event of a breakdown of the machine

1.10.5 Laptops and other easily portable equipment are particularly vulnerable to theft and damage. They should be kept in a locked cupboard when not in use and carefully protected when taken outside the office.

1.10.6 File servers must be kept in secure rooms, with access limited only to authorised individuals.

1.11 PROTECTING SOFTWARE

1.11.1 The main danger to software are:

- Unauthorised access to data
- Accidental loss of data by the user or because of machine failure
- Corruption of data by computer viruses

1.11.2 To minimise the danger of unauthorised access, users should ensure that:

- The system is returned to the password screen when leaving the office
- The machine is switched off when not in use

1.11.3 Only authorised staff should have access to computer hardware and software for the school management.

1.11.4 Passwords should be used to stop unauthorised access to information.

1.11.5 Procedures should also exist for a new password to be issued to new staff, and withdrawn when staff leave.

1.11.6 Passwords should be:

- At least six characters long and preferably contain a number
- Changed regularly (every 90 days) and as soon as a user leaves
- Not shared between users
- Not written down
- Not obvious (such as the user's telephone number)

1.11.7 School should have a recovery / business continuity plan in the event of loss of accounting or financial data. The plan should outline the need for and frequency of electronic back-up, secure storage back-ups (if possible, off-site), and manual procedures to provide support for key processes where normal system usage is not possible.

1.11.8 The following precautions should be taken to minimise any loss of data caused by machine failure or user error. (When PCs are networked and data is stored to a server, these functions should be carried out by the System Administrator)

- Give all users proper written instructions on how to use the system
- Back up all data regularly (i.e. files created by the user such as word processor documents or spreadsheet files). It is recommended that data be backed up after 8 hours' work on the machine
- If possible, keep at least three generations of back-up (i.e. the previous three back-ups). Back-up cycles should be taken daily, weekly and monthly
- Maintain a back-up of all operating software (such as Windows NT)
- Store the system disks/CDs for the applications (such as Microsoft Office) securely
- Store all back-ups away from the vicinity of the machines in a fireproof, locked cabinet or safe-preferably off-site
- Ensure that there is adequate hardware maintenance cover for critical equipment

1.11.9 To minimise the danger of data corruption by viruses and an-antivirus solution must be implemented for all networked PCs and servers. There is a continuing threat from previously undetected viruses, so staff should take the following precautions:

- Never load software without the school's IT co-ordinator's approval, including software from the internet.
- Never load any disks/CDs sent unexpectedly through the post (for example, demonstration or customer research software)
- Strictly control the transfer of software and data from one machine to another
- Never make unauthorised copies of any software
- Ensure virus-checking software is installed on all computers, and regularly updated

1.12 UNAUTHORISED USE OF SOFTWARE AND DATA PROTECTION

1.12.1 The 7th Data Protection Principle of the 1998 Act requires personal data to be surrounded by proper security. Take care at all times to ensure that staff does not render themselves liable to prosecution under the Data Protection Act.

1.12.2 Take particular care to protect data accessed or processed by 3rd parties. Any contract held with organisations or contractors authorised to process Council data should specify the security standards required. Advice on how to comply with the Act is available from Hackney Learning Trust's IT team under service level agreement arrangements.

1.12.3 Unauthorised copying of software is illegal under copyright.

1.13 INTERNET USAGE

1.13.1 Web filtering should be installed to automatically block any inappropriate websites from being accessed.

1.14 COMPUTER PRINTOUTS

1.14.1 Employees must not release information or computer data, particularly that of a personal or sensitive nature, to unauthorised persons.

1.14.2 Take care to prevent inadvertent disclosure of information, eg by ensuring that paper is suitably filed and disposed of securely.

1.14.3 Confidential waste must be shredded.

1.15 FURTHER ADVICE

1.15.1 Staff in BMBC's IT Division can provide advice under service level agreement arrangements, if required. Code Green IT Help desk can be contacted via e-mail or telephone.