SEVENOAKS DAY NURSERY

Disposal of IT Equipment Policy

Objective

This policy aims to ensure:

- Compliance with WEEE Directive (Waste Electrical and Electronic Equipment) through appropriate disposal of IT equipment.
- Compliance with the General Data Protection Regulation through secure disposal of personal data.
- Deletion of confidential or sensitive non-personal data to avoid breach of confidence, breach of contract, commercial damage.
- Deletion of software which is under licence to avoid breach of licences.
- The Nursery recovers any residual monetary value of IT equipment where appropriate.

Policy

It is Nursery policy that:

- No IT equipment (including portable devices) may be disposed of other than by the IT Manager via the processes set out in the policy. Users with equipment which needs to be disposed of should contact the IT Manager to ensure the safe disposal of the equipment.
- Prior to the disposal of computer equipment, all personal and sensitive data must be securely destroyed by a method appropriate to the risk associated with the sensitivity of data and the equipment on which it is stored as set out in the table below.
- All other data and any software licensed to the Nursery is removed prior to the equipment leaving the possession of the Nursery.
- If IT equipment is disposed of by third party contractors on behalf of the Nursery, they must adhere to the relevant standards and provide the relevant certificates of destruction and copies of waste consignment notes.

Disposal of IT Equipment

The IT Manager should be notified of any IT equipment which is no longer required. The IT Manager will then ensure that the equipment is reused or disposed of as appropriate. When disposing of equipment the IT Manager will ensure the deletion of any data and the correct disposal of equipment in accordance with this policy.

The Nursery operates a risk-based approach which differentiates disposal techniques based on the user of the IT equipment and the type of data it is likely to contain, as outlined below:

Item	Data/use	Risk	Proposed Method of data destruction	Reasons
PCs and Laptops	Standard office use	Low	Overwriting drive multiple times	Low risk of relevant data being on PC in the first place Efficient in terms of volume of equipment, staff time, physical space
	Regularly used for processing personal data or sensitive personal data eg HR, Finance, Senior Managers	Medium	Overwriting drive multiple times	Relevant data is likely to be present, therefore the need for security outweighs operational efforts required. Will ensure data is effectively not recoverable. Data on laptops should be encrypted so if recovered will still be encrypted.
	Used for processing non-personal confidential or commercially sensitive data	Medium	Overwriting drive multiple times	Relevant data is likely to be present, therefore the need for security outweighs operational efforts required Will ensure data is effectively not recoverable Data on laptops should be encrypted so if recovered will still be encrypted
	Children's records involving large amounts of sensitive personal data where data has been stored locally but not encrypted	High	Physically destroy	Impact of data loss high, could lead to court action, severe reputational damage.
Servers	Storage of personal data, sensitive personal data and confidentiality of commercially sensitive data	High	Physically destroy	Large volumes of data Mix of personal, sensitive personal, confidential, commercially sensitive data.
Other portable devices	CDs, USB sticks (pen drives), floppy disks, memory cards, tapes	Medium	Physically destroy	Simplest and most secure option With CD-Rs there is no option to overwrite For CD-R should be undertaken as soon as the data is no longer needed to be stored in that way. For other removable media should be undertaken when the storage device is no longer needed.
	Larger USB drives and external hard drives	Medium	Overwriting drive multiple times	Relevant data is likely to be present, therefore need for security outweighs operational efforts required Will ensure data is effectively not recoverable

Moving PCs

It is common practice for PCs to be moved between individuals and between rooms during their lifetime at the Nursery. There are two risks associated with the practice:

There is a risk that if a PC has been used for illegal purposes by one user, evidence of that activity will remain on the PC when it is transferred to a new user. This makes it unclear in any investigation as to who is responsible for any illegal activity.

New users may have access to confidential or personal data which had been previously stored on the PC.

In order to mitigate this risk it is the Nursery's policy that all PCs are data wiped when being permanently transferred from one individual to another.

Multi-Function devices, Photocopiers and Printers

Multi-function devices, photocopiers and printers have hard disks on which electronic copies of documents which have been photocopied, printed or scanned are stored during the operation of the device. Such hard disks must have their data removed by either data wiping or physical destruction which is dependent upon the level of risk associated with the device when it is decommissioned. As part of the contractual arrangements with suppliers, the Nursery is provided with proof of data destruction when the device is returned on termination of the lease.

Smart Phones and Tablets

All smart phones must have their data removed by being reset to factory default or by physical destruction dependent on the level of risk associated with the device and the data it has held when the device is decommissioned. If a device cannot be reset to factory default due to hardware malfunction then it must be physically destroyed.

Portable Media

Portable media which has, or had in the past, contained confidential and personal data should be disposed of in accordance with the above table.

Sale of IT equipment

Where IT equipment has a residual value the Nursery may choose to resell equipment if it is cost effective to do so. All sales will be undertaken in accordance with WEEE directives. All sales must be agreed by the IT Manager. For the sake of clarity:-

- IT equipment will not be sold until the data has been deleted as per this policy
- IT equipment that has contained sensitive or large amounts of personal data will never be sold.
- A log of all IT equipment sold should be maintained, with an overview of what data it did contain.

Scope

All Staff, contractors, partners and suppliers

This policy was adopted at a meeting of the Trustees of Sevenoaks Day Nursery CIO on 28th November, 2018.

Susan Dreksler

Chair