POLICY FOR THE DISPOSAL OF COUNCIL DOCUMENTS AND EQUIPMENT (including IT)

Date adopted: 26/10/2026

Review date: October 2028

Objective
This policy aims to ensure data protection and security is achieved through secure disposal of Council documents and equipment.

Paper Documents
Where possible, the Council will use locked waste bins for records containing personal data, and either in-house or third party cross shredding or incineration will be in place.

The Council will hold confidential waste awaiting destruction in a secure manner.

Where contracts are in place with third parties to dispose of personal data, they will provide the council with appropriate assurance that they have securely disposed of the data, for example through audit checks and destruction certificates.

The Clerk will keep a log of all equipment and confidential waste sent for disposal or destruction.

Goods and Equipment
All goods and equipment remain the property of Meltham Town Council until the Council gives permission for their disposal.

Goods and equipment that have residual value must not be disposed of without the express permission of the Council who will decide on the method of disposal.

Where the Council decides that goods or equipment are to be sold, the details of the payments, including the person(s) or organisation(s) receiving the goods or equipment, shall be recorded.

Any goods of value exceeding £500 which require disposal shall have their disposal approved by the full Council.

Upon disposal, any goods/assets of the Council will be removed from the Asset Register *[and/or any other form of additional register kept by the Council].*

IT Equipment

Any company or persons that are asked to destroy IT equipment should provide a certificate or statement that states disposal of IT Equipment has been completed and conforms to the requirement of the Council's Data Protection Policy and the UK General Data Protection Regulation 2018 and the guidance from the Information Commissioners Office (ICO).

No council owned IT equipment (including portable devices) may be disposed of outside the processes set out in this policy.

Equipment that needs to be disposed of should be stored safely until disposal takes place.

Before the disposal of computer equipment, all personal and sensitive data must be **securely** destroyed. This must be using a method appropriate to the risk associated with the sensitivity of data, and the equipment it's stored on. Complete wiping, degaussing or secure destruction of hardware (shredding) must take place.

Software licensed to the Council must be removed before the equipment leaves its possession.

Where it's physically and practicably possible or appropriate, the Council will witness the secure destruction of the equipment being disposed of.

Exceptions to the guiding principles in this policy must be documented and formally approved by the council. Policy exceptions must describe:

- the nature of the exception
- a reasonable explanation for why the policy exception is required
- any risks created by the policy exception
- evidence of approval by all appropriate parties

(Source ICO and YLCA – Feb 2024)