

Response date: 12 March 2026

You asked Money and Pensions Service the following

Please provide the following recorded information held by your department regarding assurance processes for software based data erasure of end of life IT equipment.

For clarity, this request relates solely to software based data destruction. Please exclude physical destruction methods such as shredding, crushing, degaussing or disintegration.

1. Please confirm whether departmental policy, contractual terms or internal procedures require an explicit outcome based warranty or guarantee confirming that personal data has been rendered irretrievable through software based erasure, whether carried out internally or by an external provider.
2. Where software based data destruction is performed internally, what recorded evidential assurance does the department rely upon to conclude that the final data state is irretrievable?
3. Where software based data destruction is performed by a third party provider, does the department hold recorded information demonstrating that any warranty or assurance provided explicitly extends to the software erasure method used and its claimed effectiveness? If so, please confirm the recorded nature of that verification.
4. Where no explicit outcome based warranty is required or provided, what recorded form of evidential assurance does the department rely upon to conclude that software based erasure has rendered personal data irretrievable?

Money and Pensions Service response

1. MaPS policies do not require a specific contractual warranty guaranteeing that softwarebased erasure renders data irretrievable. Instead, the applicable policies mandate the use of standardsaligned erasure methods, which provide the required level of assurance. Devices must be “securely wiped by using software which are internationally recognised and are in line with standards (Minimum of CESG Baseline Standard)” (MaPS Data Destruction Policy). Datacentre media must be erased using methods “destroyed according to NIST 80088 Guidelines for Media Sanitation” (MaPS Data Destruction Policy).
2. MaPS relies on the evidential requirements set out in our policies and procedures. These policies require the use of approved securewiping tools and the recording of sanitisation actions, including the creation and retention of Data Sanitisation or Secure Disposal Certificates. These internal records provide assurance that data has been irretrievably erased. “Data Sanitation & WEEE Recycling Certification are then sent back to MaPS” (MaPS Data Destruction Policy). Internal procedures require that “all hard disks and/or media must be securely wiped by using software which are internationally recognised” and that sanitisation is recorded as part of the disposal workflow (MaPS Data Destruction Policy).

3. MaPS relies on the evidential requirements set out in our policies and procedures. These policies require the use of approved securewiping tools and the recording of sanitisation actions, including the creation and retention of Data Sanitisation or Secure Disposal Certificates. These internal records provide assurance that data has been irretrievably erased. “Data Sanitisation & WEEE Recycling Certification are then sent back to MaPS” (MaPS Data Destruction Policy). Internal procedures require that “all hard disks and/or media must be securely wiped by using software which are internationally recognised” and that sanitisation is recorded as part of the disposal workflow (MaPS Data Destruction Policy).
4. MaPS relies on the mandatory requirements embedded in policy. These include the requirement that any data destruction is carried out using recognised securewiping methods and verified through provided certification from the supplier. These certificates provide evidence for concluding that personal data has been securely and irretrievably erased. Policies specify that “all IT equipment... must be securely wiped” using recognised software (MaPS Data Destruction Policy). The corresponding assurance is achieved through the required certificates, such as “Data Sanitisation Certificate and WEEE disposal must be obtained for any endoflife equipment destroyed professionally” (MaPS Data Destruction Policy).