Destruction of documents under the GDPR Guidelines May 2018

Disposal of confidential data

The Data Protection Act 1998 does not give any specific guidance on how to dispose of personal data. Disposal is just another step in the processing of data which requires fair and thorough attention. The seventh principle of the Data Protection Act states:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Before deciding how to comply with the seventh principle when disposing of records in any form, the data controller must consider what the data is and whether harm to the data subject, or anybody associated with the data subject, may result from its unauthorised use. You should ensure that data is disposed of in a way that creates as little risk as possible of an unauthorised third party using it.

There is no statutory guidance on the standard of shredder that should be used, but good practice concerning the standard of shredding versus the sensitivity of the information should be considered.

Non-sensitive (unclassified)
Ordinary rubbish bins should only be used for clearly 'public domain' material.

Restricted
Waste should be strip-shredded and placed in paper rubbish sacks for collection by an approved disposal firm.

Confidential
Waste should be crosscut-shredded and placed in paper rubbish sacks for collection by an approved disposal firm. The material should be pulped or burnt.

Disclosure and Barring Service
Information should be destroyed as soon as the date of receipt has been noted and the data has been viewed.
In addition, electronic memories should be scrubbed clean or destroyed. Finally, it is important to note that if you bring in a third-party data shredding service or when the shredded data is taken off-site, the responsibility for the data still lies with the data controller.