SPONSORED EDITORIAL

DEDICATED TO DESTRUCTION

NATASHA RAWLEY, THE FILE QUEEN

Wow, what a sizzler summer we are having already! Hopefully, by the time this column is printed, we are still enjoying sunny days!

In this column I want to speak to you about the importance of secure destruction. Yes, a very sexy subject! The issue is, because it's not an exciting subject, not many people are talking about it. We work with an array of legal firms and each one has their own approach to making sure that files, hard drives, USB sticks, old laptops and mobile phones are securely destroyed to prevent data breach.

But here's the question: are you dropping policies in place and just expecting everyone in the firm to follow them? Or are you being secure destruction advocates?

"What would a secure destruction advocate do?" I hear you holler. Well ...

- Regularly inspect desk bins to make sure there is no paperwork with any form of data on it being placed in normal bins.
- Inspect the paper recycling. Are people using these recycling bins for dumping sensitive info?
- Do you outsource your secure destruction or have in-house shredders? If you have an in-house shredder, is there a set process and policy that not only makes sure the shredded paper is checked after (it must be unrecognisable), but that high health and safety levels are maintained at all times? Is using the shredder listed on the new team induction tick list to make sure everyone is fully trained?
- Do you regularly have refresher training on data breaches and how to prevent them? Do these refresher courses include the whole firm? Do they include your secure destruction process and training?
- If you outsource your shredding, are you provided with a secure destruction certificate as evidence it has been shredded?
- Is the company you use audited, such as ISO 27001?
- Are you using onsite, locked secure destruction bins with your supplier or sacks? Do all members of the team know how to securely seal a sack before it is sent offsite?

> *"But here's the question: are you dropping policies in place and just expecting everyone in the firm to follow them? Or are you being secure destruction advocates?"*

As if that wasn't all enough, let's move on to the secure destruction of IT equipment. Now, most of this will be handled by your in-house or external IT provider, but as the practice manager you have an obligation to make sure this process poses no risk to your firm's reputation.

So, when a fee earner/partner is finished with a USB stick, what is the process? Do these go to IT to be wiped, or are they sent to be shredded? I know you may be a firm that doesn't allow USB technology, but what if you are sent a USB with files? What's the process?

What happens with old laptops, hard drives, or mobile phones? Is there a set process? If these are shredded and the process will have to be outsourced, who with? Are you issued secure destruction certificates? Does everyone in your practice know the procedure?

I know it's a lot to think about, but these questions are crucial in order to protect your practice reputation. LPM

ABOUT

ADDS
Saving firms from paper hell
Contact Natasha on:
0800 328 0272
www.archivestorage.net
@filequeenadds

Archive Document Data Storage

Would you like your practice to be paper lite?

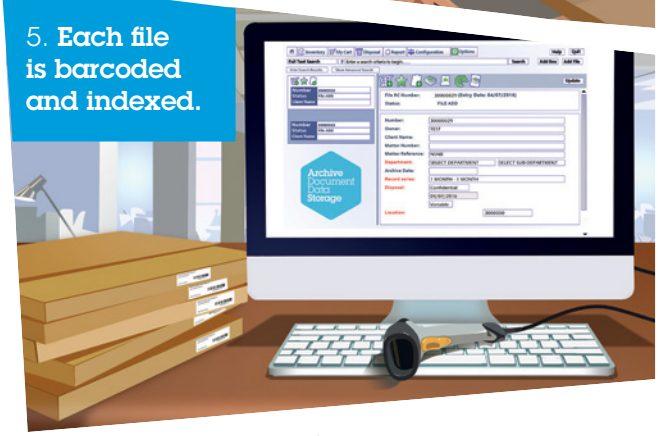
1. **Call ADDS, we can help!**

2. **Book your free consultation.**

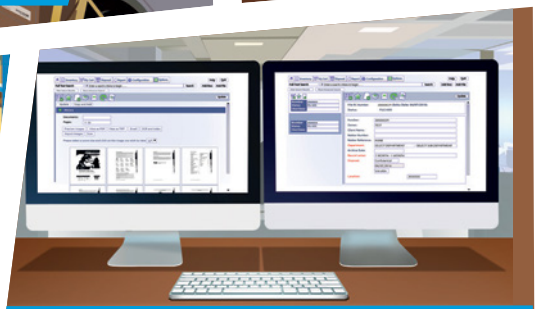
3. **We organise and pack.**

4. **Then uplift and transport to our secure records management facilities.**

5. **Each file is barcoded and indexed.**



6. **Then stored safely and securely.**



7. **You can easily request a hardcopy or electronic return via our system.**

Archive Document Data Storage

You can count on us

Contact us now for a free consultation

0800 328 0272 | www.archivestorage.net | filequeen@archivestorage.net

@filequeenadds | @filequeenadds | ArchiveDocumentDataStorage