

Shred-it Four Week Declutter Challenge

A cluttered working environment can be detrimental to your organisation's security, confidential information and reputation. Follow our four week plan with your team to recognise and remove any potential risks to help limit data exposure.

WEEK 1

WEEK 1 CHALLENGE: Organise your workspace to help protect against fraud and visual hacking.

- Remove all sensitive documents that have been left out in the open
- Put a Shred-it **Clean Desk Policy** in place so confidential material is always removed from desks or placed into locked consoles for secure destruction
- Keep work areas tidy of documents, post-it notes, business cards, access cards and removable media



MYTH

Paper really isn't a problem.



FACT

The average office worker still produces more than 10,000 sheets of paper annually.¹

WEEK 2

WEEK 2 CHALLENGE: Purge your storage room of obsolete documents to get rid of unwanted risk.

- Securely shred all paper waste in your storage room that is no longer being used
- Put a Shred-it **Document Management Policy** in place so that your employees understand what is considered confidential information.
- Review what documents should be stored in locked cabinets and what documents need to be destroyed



MYTH

All information breaches are digital.



FACT

Disclosed physical breaches, including document theft, accounted for 43% of breached assets in 2021.²

WEEK 3 CHALLENGE: Securely destroy and recycle old media and hard drives to keep private information safe.

- Call Shred-it to securely destroy and recycle your old hard drives and media. Stockpiling digital data including old hard drives, CDs and USBs, doesn't just take up space, it puts you at risk of a data breach if stolen
- Physically destroy and recycle any expired hard drives and electronic media to ensure data is 100% unrecoverable

**MYTH**

Erasing hard drives removes the data.

**FACT**

Only physical destruction ensures the data is unrecoverable.

WEEK 4 CHALLENGE: Declutter common areas and ensure confidential information stays out of the wrong hands.

- Common areas are often overlooked but they contain some surprising fraud risks
- Set reminders around the office indicating that printouts should not be left in printer trays but should be securely deposited into locked consoles if no longer needed
- No documents should be left in meeting rooms or placed in recycling bins - hold an information security training session to ensure your employees stay informed on the importance of securely destroying all expired documents
- Use our guide** to help to understand your employees' knowledge of your existing document management procedures and see if you need to refresh or retrain your employees on information security

**MYTH**

Outsourcing my document and digital destruction is too expensive.

**FACT**

Shred-it document destruction costs less than a cup of coffee a day.

¹The Benefits of Automatic Duplexing: https://www.epa.gov/sites/default/files/2013-09/documents/fec_automatic_duplexing.pdf

²<https://www.shredit.co.uk/en-gb/resource-centre/white-papers-case-studies/shred-it-data-protection-report-2021>

To learn more about best practices for information security visit shredit.ie or call 1800 747 333 (ROI) or 0800 028 1164 (NI).