

Is your office ready for the return of its employees?

Governments are beginning to recommend that businesses gradually head back to the office, bringing the much-anticipated return of in-person collaboration with colleagues. But is your office ready? With this return also comes added data security risks.

Ensure a secure return to the workplace with Shred-it.

Our steps can help your business and employees enjoy a secure return to the office.

» Encourage staff to return documents



Remote working has been a mainstay of many of our lives since the start of COVID-19. In this time, it's likely employees will have taken important documents home with them from the office or printed out potentially confidential information. Ask all employees to securely return any documents that are no longer needed to the office, so you can arrange for them to be collected and securely destroyed to help avoid the risks of a data breach.

» Declutter to get the office ready



Before employees return, get prepared and declutter documents. Do desks need clearing out? Do you have filing cabinets that haven't been organised in some time? Booking a one-time shredding service is the perfect way to declutter the office and mitigate any potential risks of a data breach. Protect your sensitive and confidential information, to start your return to the workplace as you mean to go on.

» Train employees



As employees return to the workplace now is the perfect time to train or retrain them on the best practices in secure information management and destruction. Take the time to ensure all employees understand what constitutes confidential information and how they should securely dispose of this information when it is no longer needed.

» Undertake an information security risk assessment



Awareness is the first step towards addressing and improving information security best practices. Is your company at risk of a data breach? Undertaking an information security self-assessment of office document security, document retention and employee awareness and training can help identify areas where a breach might occur.

FACT SHEET

» Establish a clean desk policy



Introducing a Clean Desk Policy will ensure that staff are disposing of and securing all unwanted sensitive information and will help mitigate the risks of a data breach.

Encourage employees to clear their desks of all papers, particularly those containing sensitive information such as personal details, account numbers and commercially-sensitive data, plus any other non-essential documents and notes (including the ubiquitous post-its) and ensure removable media, documents and notebooks are locked away at the end of the day and every time employees leave their desk.

» Introduce a document management policy



Mislaid and mishandled paper documents have been the cause of many high-profile data breaches. By implementing a Document Management Policy, you can gain

a complete picture of the documents that flow in and out of your business, what information they contain, who has access to them and how long they need to be retained.

» If in doubt, Shred-it all



The workplace is full of confidential information but determining if a document is confidential or not can be time-consuming and confusing.

So, reduce the burden on employees and help reduce the risk of a data breach with a Shred-it All Policy - where all business documents are placed in a secure, locked console and securely destroyed once no longer needed.



**For peace of mind, contact Shred-it® today
on 0800 197 1164 | shredit.co.uk**

Shred-it® is a Stericycle solution. © 2021 Shred-it® International. All rights reserved.

 **Shred-it®**