Shred-it®
A Stericycle® Solution

Secure data disposal; protect your business and the environment.

A guide to information security

We protect what matters.

Contents.

We protect what matters.

Introduction.

Safeguarding sensitive data is more than a legal obligation.

We're all familiar with GDPR legislation and constantly evolving data protection guidance but given the volume of documents that flow through a typical organisation deciding what to destroy can be a challenge. The risks can be high if customer or commercial information is stored or disposed of incorrectly, or becomes compromised.

Storage is not always the answer to staying compliant – discover the potential risks and commercial benefits around information security and how to fully realise the potential that construction companies like yours, can have as progressive force in tackling the climate crisis.

We protect what matters.

The law and secure destruction of confidential files.

Reacting quickly to changing legislation and data protection guidance can be challenging. The more information we hold on to, the more burdensome it can be to stay compliant.

New Bills and evolving regulatory guidance around the handling, storing and protection of EU and UK citizens' personal data, can quickly affect internal document management processes.

▶ The Data Protection Act

▶ UK General Data Protection Regulation

▶ The Information Commissioner's Office

▶ Data Subject Access Requests

Delaying the destruction of unneeded documentation, hanging-on to papers and storing them in perpetuity or disposing of papers in recycling bins may leave your business unintentionally open to data breaches and monetary penalties.

The Information Commissioner's Office (ICO) recommends secure shredding to destroy paper documents. Working with information destruction professionals will help make sure that your business benefits from a secure chain of custody for your sensitive information alongside compliance with evolving data protection rules.

We protect what matters.

Understanding the risks.

Data breaches and unsecure recycling can have a significant impact on your sites.

Financial Losses

Data breaches can lead to financial losses due to the cost of notifying affected individuals; ICO monetary penalties; and complying with regulatory requirements.

Reputational Damage

Alongside business disruption, a data breach could reduce client confidence and cause reputational damage.

Legal Liability

Your sites may be liable to pay compensation to data subjects as a result of a data breach.

Insecure Disposal

Leaving documents in an unsecure recycling bin may seem environmentally-aware but important and confidential information can be jeopardised if it is retrieved from the bin.

We protect what matters.

For service, please contact us at:
0800 028 1164

Data security mistakes that can compromise confidential information.

Confidential information stored on blue prints, customer forms, contracts and inspection reports should be safeguarded against malicious outsiders and destroyed when no longer needed.

Leaving Data Exposed
Always protect and shield private information when it's visible in public spaces - for example, unfiled sensitive information left on desks and laptop screens clearly visible to others.

Stockpiling Hard Drives
Instead of storing or discarding your old hard drives, USBs, CDs etc, shred and destroy your digital and electronic media securely so any data recovery is impossible.

Office Shredders
The hidden security, productivity and safety concerns of a DIY approach include maintaining costly commercial-grade equipment; employees having access to highly sensitive materials which they may not normally have permission to access; and documents not being completely destroyed.

Lacking Employee Training
According to research[1], 48% of the small business leaders said that employee error is a main source of data breaches - help employees better understand their role in helping your firm remain secure.

We protect what matters.

Files on the move: risks outside the office.

Hybrid working, commuting between constructions sites and traveling to client offices add additional security and sustainability concerns to existing information management policies and practices.

Independent research for Shred-it[2] for example shows that employees working from home could be risking client data and commercial secrets leaking out due to lax security in their home office or workspace.

Not recycling and securely shredding documents when working outside the office may also have an impact on your corporate green initiatives and net zero targets.

Survey results revealed:

88% of respondents deal with confidential papers, but...	**24%** do not always follow their workplace policy on destroying confidential information when working from home.	**50%** of respondents said that other people in their home could see confidential information.	**18%** don't recycle shredded work documents when at home and/or just put documents in the bin.

We protect what matters.

Challenges facing businesses

Businesses are finding it increasingly challenging to protect sensitive information and are worried about the impact a data breach could have on their customers.

An independent research report examining the perception of 500 business leaders has highlighted concerns about the protection of sensitive data and the risk of breaches.

When it comes to GDPR and regulatory compliance, respondents indicate they are finding data protection regulations and compliance complex areas to navigate but acknowledge a critical need to improve data protection.

Survey results revealed:

90%
of respondents find it challenging to protect their company's sensitive data.

41%
of respondents have experienced a data breach at their company.

62%
fear not enough focus is given on keeping physical information secure.

72%
are afraid of the impact a data breach will have on their customers.

Research for Shred-it carried out online by Opinion Matters between 24/08/2023 and 30/08/2023 among 502 business leaders in the UK aged 18+ i.e. owners, executives, C-level, VP, Director+ or equivalent in companies of over 50 employees.

We protect what matters.

Sustainability: aligning data protection with net zero targets.

Most businesses have targets to take action on climate change and support in reaching net zero. To achieve these targets it is crucial to use secure and sustainable practices across all aspects of business operation.

Sustainability is firmly on the national agenda and the public is increasingly looking to organisations to help tackle major environmental issues.

The Climate Change Act 2008 commits to:

▶ reducing greenhouse gas emissions to net zero by 2050

▶ reducing emissions by at least 68% by 2030 and 78% by 2035

The construction sector has a significant role to play in how we can all help to meet national net zero targets. Through collective priority setting, the sector is looking at low carbon solutions, modern methods of construction and embracing the circular economy to drive change - on work sites, in the office and across supply chains.

Many construction companies now have ESG policies which include details of the actions they are taking to drive improved environmental outcomes.

Secure data destruction and recycling complements sustainability initiatives by ensuring that shredded paper gets into the circular economy. Organisations can stay compliant with data protection regulations and demonstrate their Scope 3 emissions associated with paper collection and shredding under the category Purchased Goods and Services.

We protect what matters.

Practical steps: what you can do now.

Take immediate steps towards protecting confidential information and embed sustainable practices in your organisation – explore the following actionable items:

Privacy Notice

Develop a comprehensive privacy notice that outlines your data protection commitments and informs individuals about their rights. Explain how and how long personal data will be retained before being disposed of/destroyed – including data contained in paper records.

Retention Policy

Address physical records and explain the process for deletion/destruction.

Workplace Policies

Implement robust workplace structures that promote information security awareness among your employees and foster a culture of responsibility and vigilance. Consider the need for policies that mitigate security risks associated with physical records, such as clean desk policies and document management policies.

Secure Storage

Safeguard sensitive information by utilising secure storage solutions such as locked cabinets, restricted access areas, and encrypted digital storage. Consider risks presented by different media, such as paper vs. hard drives.

Staff Training

Invest in comprehensive staff training programs to educate employees about information security best practices. Empower your workforce to be the first line of defence and ensure policies and standards are implemented and adhered to.

Secure Destruction

Partner with a trusted secure destruction service provider, such as Shred-it. Ensure that your confidential materials are handled securely, destroyed effectively and recycled responsibly.

We protect what matters.

How a secure destruction service provider can help.

Partnering with a secure destruction service provider such as Shred-it, can help you discover best practices that align with your organisation's commitment to compliance and sustainability in a cost effect and secure way.

Regular or one-off collections

Onsite or offsite shredding

Secure chain of custody

Certificate of Destruction

All shredded paper is recycled

We protect what matters.

Shred-it®
A Stericycle® Solution

Call **0800 197 1163**

Visit **shredit.co.uk**

Contact us today and take your next step towards building a resilient information security framework that helps safeguard your organisation's reputation, maintains trust, ensures compliance and contributes to your net zero journey.

[1] Shred-it 2022 Data Protection Report

[2] Shred-it Data on File, 2022

We protect what matters.