WITHOUT ONE YOU COULD BE
PAYING A HIGH PRICE

SIA
Sensitive Information Audit
by Fellowes

Email us for more information or to book your
Sensitive Information Audit
salesadmin@fellowes.com

www.fellowes.com

SIA
Sensitive Information Audit
by Fellowes

Fellowes Brands

WITH A SENSITIVE INFORMATION
AUDIT YOU HAVE
NOTHING TO LOSE

SIA
Sensitive Information Audit
by Fellowes

SIA
Sensitive Information Audit
by Fellowes

It's crucial for organisations to take care of confidential information to comply with the Data Protection Act - and to protect their business. Data held by an organisation must be kept secure and disposed of safely; ensuring confidential and personal information is destroyed.

If it's not disposed of correctly, your organisation could be paying a very high price. The Information Commissioners Office (ICO) can issue fines of up to £500,000 and with the new GDPR it could be up to €20million for each time the law is breached. And where FSA regulations are in place, the fines are unlimited.

These penalties are damaging enough. But there could be far more reaching consequences on your reputation. In fact, when confidential material falls into the wrong hands, the damage incurred can often be irreparable.

There are three main reasons for undertaking a Sensitive Information Audit

1. To ensure your organisation has a robust information protection policy for:
   - Managing records
   - Protecting sensitive information
   - Destroying confidential documents

   In accordance with the Data Protection Act
2. To assess the efficiency of your existing information protection systems
3. To identify any cost savings that can be made on your existing information systems

Fellowes Brands

Research proves that employees are not taking enough care of company information. Confidential data about themselves, their business and their clients is frequently in plain view of prying eyes. On desks… on photocopiers… on screens… in meeting rooms. And sensitive information that's out in the open is open to exploitation.

Every organisation has a legal responsibility to safeguard sensitive information and dispose of confidential material securely. The organisation is also responsible for any confidential material that's taken outside its premises by any of its employees. This includes both hard copy documents and anything that can be viewed on a computer, laptop or mobile device.

A laptop stolen from the car of a Staffordshire University employee in 2014 contained the details of 125,000 students and applicants.

In 2007, HM Revenue & Customs lost two CDs containing 25 million child benefit claimants.

Aberdeen City Council was fined £100,000 when an employee posted confidential information relating to vulnerable children online. This resulted in the council agreeing to work with the ICO to improve its homeworking policies to comply with the Data Protection Act.

The personal data of 11 million savers was put at risk when the laptop of a Building Society employee was stolen. The FSA eventually fined the Nationwide £980,000, which is the largest sum ever imposed for data loss in the UK.

In 2013, NHS Surrey was fined £200,000 after losing sensitive information about 3,000 patients.

An employee of a Scottish council took details of an adoption case home and they were stolen. The regulator came down heavy on the council for repeatedly failing to train staff on data protection.

Source: ico.gov.org

How secure is your desk?

Failing to comply with the Data Protection Act is a criminal offence, and the commissioner can impose a penalty of up to

€20 Million

One small mistake can result in a hefty fine and a damaged reputation…