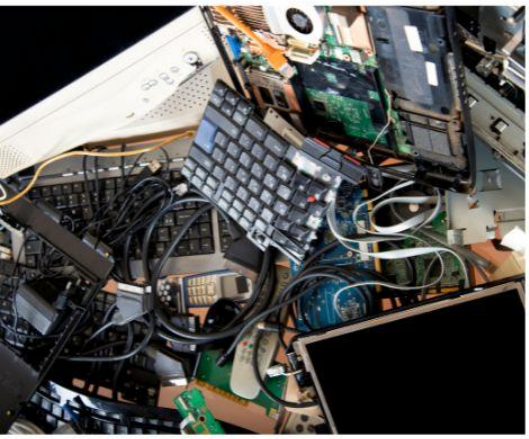

BS EN 15713:2023 – **A Complete Guide**

Introduction

In today's fast-paced business world, data and information is key to the success of most organisations. As such, it is essential for businesses of all sizes to protect their confidential data, including customer details, employee records and finance and accounting information. With legislation now imposing financial penalties on companies that fail to keep their data safe, there has never been a better time to put best practice in to place to ensure your confidential data is protected right through to the end of its life cycle.

As a European standard, BS EN 15713 is the authoritative document on data destruction. It sets out the measures that organisations should take to maintain the security of confidential data and provides recommendations relating to the management and control of collection, transportation and destruction of confidential material to ensure such material is disposed of safely and securely. Developed by the European Committee for Electrotechnical Standards (CENELEC), BS EN 15713 should be the first port of call for any organisation looking to improve its secure data destruction processes.

The standard places emphasis on guaranteeing the secure destruction service, ensuring that staff who are involved in the confidential shredding business are security vetted to BS 7858, vehicles are secure, premises are alarmed and monitored and confidential material is processed and destroyed correctly. BS EN 15713 is a complete document and deals with much more than shredding sizes as it provides the complete secure solution. This document outlines the requirements of the standard.

Glossary

Confidential Material – this can be information stored or printed on paper records, computer media, digital memory, hard discs, optical discs, smart cards, magnetic tape. This also means commercial and intellectual products and property etc. The term 'confidential' does not refer to UK Government security classifications, but is a generic industry standard term.

Information Destruction – the destruction (shredding or disintegration) of confidential material to a state that is unrecognisable and compliant with the Data Protection Act 2018.

Information Governance – the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.

Data Protection Act 2018 – if you handle personal information about individuals, you have a number of legal obligations to protect that information. Principle 6 of the Act states that appropriate technical and organisational measures shall be taken against unauthorized processing of personal data.

General Data Protection Regulations (GDPR) - a legal framework that sets guidelines for the collection and processing of personal information of individuals which came into effect across the EU on 25th May 2018.

BS EN 15713 – Approved European standards for Information Destruction, that supersedes any other national standards. Providing secure information governance from collection, destruction and recycling. This standard must be incorporated within a robust quality management system and audited through and audited through a UKAS approved body to ensure compliance.

BS EN ISO 9001, ISO 14001 and 27001 – UKAS approved Quality management, Environmental and/or Information Security systems ensures a service provider belonging to the BSIA operates to the highest standards incorporating the BS EN 15713 and is audited yearly to ensure quality procedures are maintained.

DIN (Deutsches Institut für Normung) – the German national organisation for standardisation and is that country's ISO member body. DIN is a Registered German Association for standards. DIN standards relating to data destruction are not appropriate for use within the UK.

National Protective Security Authority (NPSA) – High security – The NPSA protects national security by providing protective security advice to the UK's national infrastructure as defined by the Government as: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends".

The National Cyber Security Centre – The NCSC is a part of GCHQ. It protects the vital interests of the UK by providing policy and assistance on the security of communications and electronic data, working in partnership with industry and academia. NCSC is the UK Government's National Technical Authority for Information Assurance (IA). Core customers are the UK's central government departments and agencies, and the Armed Forces. It also works with the wider public sector, including the Health Service, law enforcement and local government, as well as all essential services that form the UK's Critical National Infrastructure, including power and water.

Cabinet Office Government Security Classifications Policy – High security - The Cabinet Office issued the Government Security Classifications Policy, which took effect in April 2014 replacing the old Government Protective Marking Scheme.

TOP SECRET. The Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

SECRET. Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

OFFICIAL. The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. A limited subset of **OFFICIAL** information that would have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media is classified '**OFFICIAL**-**SENSITIVE'**.

Most of a public authority's data will fall into the OFFICIAL Category (subject to individual risk assessments) and can be treated by a company providing a service compliant to BS EN 15713, who also has a robust BS EN ISO 9001 quality control system, demonstrating good compliance. If further guidance is required within the public authorities this should be obtained from their internal security controller, and for further guidance refer to the Cabinet Office website.

Note: It should be noted that BS EN 15713:2023 incorporates the complete information destruction process, from collection, destruction and recycling and as a European Standard BS EN 15713 takes precedence over other national standards. This guide is only an aide-memoire and does not replace any of the requirements of the standard.

1. Defining Protection Class and Security Level

The standard requires the Data Controller to define the protection class and security level of material. There are three classifications;

Routine Confidential (RC) – normal protection level for internal data; the most common classification of data intended for large groups of people

Official Sensitive (OS) – the information is restricted to a small group of people

Highly Sensitive (HS) – the information is restricted to a very small group of named persons

Where a protection is not defined the UK Information Destruction Industry aligns behind providing a service in line with Routine Confidential. This document gives an overview of the minimum requirements needed to provide a service at Routine Confidential, for further information on higher security classes please speak with a member of the BSIA Information Destruction Section as all our members operate in line with BS EN 15713:2023.

For material category P (original size data carriers such as paper) and F (miniaturized form data carrier such as microfilm), mixing and compacting can be used to increase the security level to the next higher level where material being mixed is at least 100kg. For industrial shredding services, mixing and compacting of material to increase the security level is standard practice across the UK.

2. Confidential destruction premises

BS EN 15713 states that all premises carrying out information destruction should:

- Have an administration office where necessary records and documentation are kept for conducting business.
- Be separated from other business or activities on the same site.
- Have an intruder alarm installed to BS EN 50131-1, monitored by an alarm receiving centre.
- Have a video surveillance system (VSS) with recording facilities that monitors the secure area entrances, unloading, storage and processing areas. The images should be retained in line with the company's retention policy (or similar).
- Destruction takes place within a secure area with protective security measures in place.

3. Contracts

The standard also requires that the following legal agreements regarding responsibility should be in place:

- A written contract covering all transactions should exist between the client and the organisation.
- The contract should state the protection class of the confidential material being processed, the security level assigned to the material and whether mixing and compacting is allowed by the Data Controller to increase the security level.
- Sub-contracted work should only be allocated to identified companies following the recommendations in BS EN 15713:2023.
- In every case, clients should be informed if sub-contractors are used. The client, as data

controller, should:

- Choose a data processor providing guarantees in respect of technical and organisational security measures.
- Take reasonable steps to ensure compliance with these measures.

- Evidence of destruction will be confirmed to the client by the issue of a Certificate of Destruction

4. Personnel

BS EN 15713 states that all personnel involved in the destruction of confidential data should:

- Be security vetted in accordance with BS 7858, which includes a Disclosure and Barring Service (DBS) check.
- Have signed a Deed of Confidentiality prior to commencement of employment.
- Shall be trained in the processes required, relevant to the material Protection Class, with training records kept and refresher training provided.

5. Collection and retention of confidential material

The standard requires information destruction companies to employ the following measures when collecting confidential data:

- Confidential material to be collected should remain protected from unauthorised access from the point of collection to completion of destruction.
- Collection should be made by suitably trained staff, wearing company-branded clothing and carrying photographic identification.
- The destruction of confidential material shall take place within one working day from arrival at the destruction centre or in any event, within 96 hours from collection from the client premises, where shredding is taking place off site at a destruction facility.

6. Vehicles (off site)

Vehicles collecting confidential data for destruction off site should:

- Be either box bodied or have a demountable container.
- Where a curtain side vehicle is used, material should be transported within a suitable sealed secure container.
- Be able to communicate with home base by radio or telephone.
- Be fitted with a remote tracking device
- Be fitted with an audible anti-theft alarm or immobilizer, which shall be armed when unattended.
- Be closed and locked/or sealed during transit.

7. Vehicles (on site)

Vehicles destroying confidential data on site should:

- Be box bodied.
- Be fitted with lockable and/or sealable doors.
- Be able to communicate with the home base by radio or telephone.
- Be fitted with an audible anti-theft alarm or immobilizer, which shall be armed when unattended.
- Not be left unattended when unprocessed material is onboard.
- Be fitted with a remote tracking device.

8. Destruction Equipment

BS EN 15713 requires the following to be in place regarding destruction equipment being used:

- Material output from the destruction equipment shall be sample tested to ensure it can meet the requirements of the destruction outcome.
- Destruction equipment shall be regularly serviced and maintained by a competent person.
- There should be a contingency plan in place for redundancy/failure of destruction equipment.

9. Environmental issues

BS EN 15713 requires the following environmental measures to be taken when destroying confidential waste:

- 'Where practicable, and with safety as a priority, end product materials should be managed by application of the waste hierarchy. In many cases there will be opportunities to recycle materials which is preferable to disposal. If recycling is not practicable, the cost and convenience of other methods should be taken into account. Landfill should only be used where no other method of disposal is practical.
- Waste Transfer Notes should be issued for each consignment, or annually for regular scheduled collections.

10. Customer due diligence

It is recommended that customers carry out due diligence directly with their existing or prospective destruction company, taking into account the above points and also the below:

- **Physical check** of destruction process, equipment, and vehicles.
- **Duty of Care audit to ensure environmental regulatory compliance:** Destruction companies must be registered with the Environment Agency and have a Waste Carriers Licence, and if processing off site an Environmental Waste Permit or registered exemption. Copies of certificates should be provided.
- **https://www.gov.uk/guidance/access-the-public-register-for-environmental-information**
- **Vehicle Operating Licence:** destruction companies collecting confidential material must have an approved Driver and Vehicle Standards Agency licence if operating commercial vehicles. **www.gov.uk/government/organisations/driver-and-vehicle-standards-agency**
- **Information destruction BS EN 15713 compliant:** Customers should ask for an up to date copy of the company's BSIA membership certificate. Please check **https://www.bsia.co.uk/id-members/** for up to date contact details for each member.
- **Insurance minimum cover** of £5,000,000 public and products liability and £10,000,000 employers liability together with a minimum of £1,000,000 professional indemnity insurance.
- **Health and safety policy, risk assessments and safe operating procedures** should be provided to customers to ensure safe operating standards and welfare.
- **BS EN 15713:2023** introduces business continuity management, risk and vulnerability assessments and compromise management procedures in place to deal with the possibility of a deliberate security breach. A further introduction, allied to GDPR compliance, is the obligation for an information security policy.

11. Information Destruction Matrix

11.1 Assignment of security levels and protection classes

Protection class	Security levels						
	1	2	3	4	5	6	7
RC	x	x	x				
OS			x	x	x		
HS				x	x	x	x

11.2 Categories of confidential and sensitive material

EN 15713 Material Categories	Category description	Examples of confidential and sensitive material
P	Information in the original size data carriers	Paper, plans, documents, drawings, film, printing plates, dental impressions, etc.
F	Information in miniaturized form data carrier	Microfilm/microfiche etc.
O	Optical data carriers	CD/DVD etc.
T	Magnetic data carriers	Floppy discs, ID cards, magnetic tape cassettes etc.
H	Hard drives with magnetic data carriers	Hard drives
E	Electronic data carriers	Memory sticks, chip cards, solid-state drives, mobile communication equipment, digital door locks, electronic key cards, etc.
M	Product Destruction	Contraband or counterfeit goods, defective and obsolete products, mechanical keys and locks. Corporate or branded clothing and uniforms.

11.3 Destruction outcomes

Please look at Tables under Annex A of BS 15713:2023 for full destruction outcomes. For Paper, please see example outcomes table below at security level P-1.

Information in the original size e.g. paper, film, printing plates		
Security level	**Condition, shape and size after destruction**	**Tolerance**
P-1	Particle size ≤ 2000 mm^2 or Strip width ≤ 12.0 mm Unlimited strip length	10% of the material may exceed the specified particle size but shall not be more than 3800 mm^2 in size.

BS EN 15713:2023 incorporates the complete destruction process and should not be viewed as only providing shred sizes. As a European Standard BS EN 15713 takes precedence over other national standards such as DIN (Deutsches Institut für Normung).

It should also be noted that, as a general rule, the smaller the shred size required (output), the slower the throughput (tonnage per hour) achieved and therefore the higher the cost to achieve that particular output. Consequently, self-classification by the Data Controller, along with guidance from other informed bodies or associated third parties is the most logical approach to specifying desired shred sizes. For example, a book publisher creates a large surplus of a publication that they want destroyed. In this case a 25mm cutting width is more than adequate to render the product useless and to specify a smaller output would not be sensible commercially. The same principle applies to other products such as uniforms.

The BSIA supports this 'risk management' versus 'desired outputs' approach to classifying products & data for destruction. With paper still representing a high proportion of what currently needs to be securely and safely destroyed, the destruction industry in general, including destruction equipment manufacturers, service providers and clients/customers, are aligning with the choice of P-2 as being the Security Level most appropriate for Routine Confidential material destruction.

12. Useful websites

British Security Industry Association
www.bsia.co.uk/sections/information-destruction

Information Commissioner's Office (ICO)
www.ico.org.uk

Environment Agency
www.gov.uk/government/organisations/environment-agency

Driver and Vehicle Standards Agency
www.gov.uk/government/organisations/driver-and-vehicle-standards-agency

British Standards Institute (BSI)
www.bsigroup.co.uk

National Protective Security Authority
www.npsa.gov.uk

Cabinet Office Government Security Classifications Policy – high security
www.gov.uk/government/publications/government-security-classifications

The National Cyber Security Center (NCSC)
www.ncsc.gov.uk

British Security Industry Association
t: 01905 342 020
e: info@bsia.co.uk

This guidance document was created by the Information Destruction section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

The BSIA Information Destruction (ID) Section consists of companies that securely destroy a range of confidential information, including paper, DVDs and computer hard-drives. The section also destroys items that could potentially cause problems if they fall into the wrong hands, such as branded products and uniforms.

The section highlights the importance of information destruction for businesses and the benefits of using a quality supplier. With identity fraud rising, sensitive information and data needs to be destroyed properly otherwise confidential details can be put at risk.

The ID section's work is particularly relevant to the Data Protection Act. Every Data Controller using an information destruction company is required to choose a supplier which provides sufficient guarantees of security measures, including destruction being carried out under contract and evidenced in writing. All BSIA Information Destruction companies offer this quality guarantee.

This guidance document is for use by any interested party who provides or uses a destruction company.

Section members work to a European Standard for the secure destruction of confidential material (BS EN 15713) as part of their ISO 9001 or ISO 27001 inspection.

About **the BSIA**

This guidance has been produced by the Information Destruction Section of the BSIA.

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.