

Data Destruction Policy



Purpose:

Gemini Print Solutions is committed to ensuring that all personal and sensitive data, whether in physical or electronic form, is securely destroyed when no longer required, in accordance with UK GDPR and best industry practices. This policy applies to all employees, contractors, and third-party processors handling our data.

1. Scope

This policy covers:

Physical data: paper documents, printed materials, and any other tangible records containing personal or sensitive information.

Electronic data: computer files, emails, databases, backups, removable storage devices, and other digital records.

2. Principles

Data will be retained only as long as necessary for operational, legal, or contractual purposes.

All destruction of data must render it completely irrecoverable.

Data destruction methods must comply with UK GDPR, the Data Protection Act 2018, and industry standards such as ISO/IEC 27001:2013.

3. Procedures

3.1 Physical Data

Shredding: All confidential documents will be shredded using cross-cut or micro-cut shredders.

Disposal: After shredding, waste will be recycled or securely disposed of via authorised contractors.

Storage: Sensitive physical records awaiting destruction will be kept in locked, access-controlled storage.

3.2 Electronic Data

Overwriting: Electronic files will be securely erased using industry-standard data wiping software.

Data Destruction Policy



Deletion of media: Hard drives, USBs, CDs, and other storage media containing personal data will be physically destroyed if they cannot be securely wiped.

Cloud & backups: Data stored in cloud services or backups will be permanently deleted in accordance with the provider's secure deletion procedures.

4. Roles & Responsibilities

Data Protection Officer (DPO): Steve Cropper oversees compliance, maintains records of destruction, and audits the destruction process. He can be contacted at s.cropper@geminiprintsolutions.co.uk.

Employees & Contractors: Must follow this policy and report any breaches or incidents to the DPO.

Third-party Processors: Must provide evidence of secure destruction when handling Gemini Print Solutions' data.

5. Record-Keeping

A log of all destroyed data, including date, method, type of data, and responsible party, will be maintained for accountability and audit purposes.

6. Policy Review

This policy will be reviewed annually or sooner if there are changes to legislation, operational requirements, or technology affecting secure data destruction.

A handwritten signature in black ink, appearing to read "Steve Cropper".

Steve Cropper

Director

Updated: 12th January 2026

Next Review Date: 12th January 2027