jrhsupport

DATA DESTRUCTION POLICY

DATA DESTRUCTION POLICY

Policy Statement
JRH Support is committed to protecting the privacy and security of all personal and sensitive data handled in the course of providing social care services. This Data Destruction Policy outlines the procedures for the secure and irreversible destruction of data, ensuring compliance with relevant data protection legislation (e.g., UK GDPR, Data Protection Act 2018), ethical guidelines, and internal data retention schedules.

Scope
This policy applies to all employees, volunteers, contractors, and any third parties who have access to data held by JRH Support. It covers all forms of data, including:

- Electronic data (e.g., on computers, servers, mobile devices, cloud storage, external drives)
- Paper records (e.g., service user documentation, administrative documents)
- Audio and video recordings

Principles of Data Destruction
- Necessity: Data will only be destroyed when it is no longer required for its original purpose, legal obligations, or legitimate business interests, as determined by the Record Retention Policy.
- Security: Data destruction will be carried out in a secure manner to prevent unauthorised access, disclosure, or reconstruction of the data.
- Irreversibility: Destruction methods will ensure that the data is permanently irretrievable.
- Documentation: All data destruction activities will be documented.
- Compliance: All data destruction will comply with applicable laws and regulations.

Record Retention Schedule
JRH Support maintains a separate Record Retention Policy which specifies the retention periods for different categories of data. Data will be marked for destruction once its retention period has expired. This schedule is reviewed annually and updated as necessary.

Methods of Data Destruction
The method of data destruction will depend on the type of data and the medium on which it is stored.

Electronic Data Destruction
- Hard Drives/SSDs (Computers, Servers):
    - Secure Erase Software: For re-purposed or end-of-life devices, industry-standard data erasure software (e.g., satisfying DoD

5220.22-M or equivalent) will be used to overwrite data multiple times.
    - Physical Destruction: For drives that are faulty or cannot be securely wiped, physical destruction methods such as degaussing (for HDDs) or shredding/crushing will be employed by a certified third-party provider.
- USB Drives/SD Cards/Other Portable Media:
    - Secure erasure software where possible.
    - Physical destruction (shredding, crushing) for media that cannot be reliably erased.
- Mobile Devices (Phones, Tablets):
    - Factory reset combined with data overwrite apps where available.
    - For devices being disposed of, consider professional data wiping services or physical destruction.
- Cloud Storage:
    - Data stored on cloud platforms will be deleted through the platform's provided mechanisms. Confirmation of deletion will be sought from the cloud provider where possible. It is understood that data may reside on backups for a limited period; this will be factored into our retention schedule.
- Emails and Digital Documents:
    - Permanently delete from email clients and trash folders.
    - Permanently delete from shared drives and individual computer recycle bins.

Paper Record Destruction

- Shredding: All paper records containing personal or sensitive data will be cross-shredded using a shredder that meets at least a P-4 security level (DIN 66399 standard).

Audio and Video Recordings

- Digital recordings will be securely deleted using methods equivalent to electronic data destruction.
- Physical media (e.g., tapes, CDs, DVDs) will be physically destroyed (shredded, broken).

Responsibilities

- Data Protection Officer (DPO) – General Manager: Overall responsibility for the implementation and oversight of this policy and the Record Retention Policy
- All Employees: Responsible for understanding and adhering to this policy and the Record Retention Policy when handling and disposing of data.
- General Manager: Responsible for overseeing the secure disposal of paper records and managing confidential waste contractors.

Procedures for Data Destruction

1. Identify Data for Destruction: Regularly review data against the Data Retention Schedule.
2. Authorisation: The DPO or a designated manager must authorise all data destruction, particularly for large datasets or critical records.
3. Perform Destruction: Execute the appropriate destruction method as outlined in Section 5.
4. Verify Destruction: Where possible, verify that the data has been irrevocably destroyed. For professional services, obtain a certificate of destruction.
5. Document Destruction: Record the following details in a Data Destruction Log:
    - Date of destruction
    - Type of data destroyed (e.g., "Client file of John Doe," "Server hard drive")
    - Medium of data (e.g., "Paper," "HDD," "USB drive")
    - Method of destruction (e.g., "Cross-shredded," "Secure erase software - DoD 5220.22-M," "Professional shredding service - Certificate #ABC123")
    - Name of person performing/overseeing destruction
    - Any certificate of destruction reference number

Third-Party Data Processors

If engaging third-party processors (e.g., cloud providers, IT support, confidential waste services), JRH Support will ensure that:

- Contracts include clear clauses regarding data destruction, requiring compliance with this policy and relevant data protection laws.
- Due diligence is performed to ensure the third party employs appropriate security measures for data destruction.
- Certificates of destruction are provided by third parties where applicable.

Policy Review

This Data Destruction Policy will be reviewed at least annually, or sooner if there are changes in legislation, technology, or business practices.

Breach Reporting

Any accidental or unauthorised disclosure or access to data during the destruction process must be reported immediately as a potential data breach

Paul Battershall
General Manager