WESTON ARK CHARITY - DATA PROTECTION POLICY

TRUSTEE-APPROVED POLICY

Weston Ark | The Hughenden Centre, 25 Hughenden Road, Weston-super-Mare, BS23 2UR
07778 378216 | info@westonark.org.uk | www.westonark.org.uk

Document Version: 1.1
Approved: November 2026
Next Review: November 2027

Our Commitment

Weston Ark Charity is a Christian organisation demonstrating God's love through practical support for low-income families and individuals. Operating from the Hughenden Centre, our services include the Ark Café and venue hires, alongside supporting a Weston Foodbank outlet operated by dedicated Foodbank volunteers.

We are committed to protecting personal data entrusted to us by service users, volunteers, staff, donors, and partners. Data protection reflects our core values of respect, trust, and care for every individual we serve.

Legal Framework

This policy ensures compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025 (DUAA) - incorporating recent changes
- Privacy and Electronic Communications Regulations 2003
- Information Commissioner's Office (ICO) and Charity Commission guidance

Weston Ark is the Data Controller for all personal data we process and is legally responsible for ensuring compliance.

Key Definitions

- Personal Data**:** Any information relating to an identifiable living person (names, contact details, financial information, venue bookings)
- Special Category Data: Data such as health, religious beliefs or ethnicity requiring an additional legal condition. Financial hardship is sensitive but is not, by itself, special category data.
- Processing**:** Any operation with data (collection, storage, use, sharing, deletion)
- Data Subject**:** The individual whose personal data we hold

Data Protection Principles

Lawfulness, Fairness, Transparency**:** We process data lawfully with clear privacy notices explaining how and why we use information.

Purpose Limitation**:** Data collected for specific purposes only. Foodbank referral data will not be used for fundraising without separate consent.

Data Minimisation**:** We collect only necessary information. Simple venue enquiries require only name and contact details; debt advice requires comprehensive financial information.

Accuracy**:** We maintain accurate, up-to-date information and provide opportunities for individuals to correct their data.

Storage Limitation**:** Data retained only as long as necessary according to our retention schedule, then securely destroyed.

Security**:** Appropriate technical and organisational measures protect against unauthorised access, loss, or damage.

Accountability**:** We demonstrate compliance through policies, training records, and documented procedures.

Lawful Basis for Processing

Consent**:** For non-essential activities like promotional materials featuring service users. Must be freely given, specific, informed, and easily withdrawable.

Contract: For venue hire, ticket purchases and employment contracts. Necessary administration of other attendees uses documented legitimate interests.

Legal Obligation: For Gift Aid claims, safeguarding reporting, and Charity Commission requirements.

Vital Interests: Only for life-threatening emergencies where consent cannot be obtained.

Legitimate Interests: For essential charity operations after conducting Legitimate Interests Assessments. The new "soft opt-in" for charitable direct marketing applies to new supporters only where proper opt-out mechanisms are provided.

Recognised Legitimate Interests: Under the 2025 Act, certain activities (crime prevention, safeguarding, emergency response) are automatically recognised as legitimate without full balancing tests.

Data Security and Technology

Approved Systems: Use charity-managed Microsoft 365 for communications and records, Microsoft Azure for the website, Stripe for online payments and HallMaster for room hire. Personal email and storage accounts are prohibited.

Security Requirements:

- Strong, unique passwords on all accounts
- Two-Factor Authentication mandatory on all Microsoft 365 accounts
- Full-disk encryption on portable devices
- Regular software updates and antivirus protection
- Locked filing cabinets for physical records
- Secure disposal of confidential materials

HallMaster System: Used for venue bookings with appropriate data processing agreement in place.

Website Access: Only the Technology and Systems Lead edits the CMS; trustees authorise access changes. Organisers see only necessary event data. Use individual accounts and multi-factor authentication; review access quarterly and remove it when duties end. Protect credentials, ticket links and exports.

Website Security: The Technology and Systems Lead maintains updates, logs, protected backups and recovery instructions, tests restoration quarterly and reports breaches immediately. Develop with test data. Check content accuracy, accessibility, permissions and expiry before publication.

Individual Rights Under UK GDPR

Data subjects have the right to:

- Be Informed: Clear privacy notices at point of data collection
- Access: Request copies of their personal data (Subject Access Request)
- Rectification: Have inaccurate data corrected
- Erasure: Have data deleted in certain circumstances
- Restrict Processing: Limit how their data is used
- Data Portability: Obtain data in portable format
- Object: To processing based on legitimate interests or direct marketing
- Protection from Automated Decision-Making: Safeguards against purely automated decisions

Making Requests: Contact the Data Protection Lead verbally or in writing. We respond within one calendar month.

Data Breaches

Immediate Response: Any suspected breach must be reported immediately to the Data Protection Lead. First priority is containment and risk assessment.

ICO Reporting: Breaches likely to result in risk to individuals' rights must be reported to ICO within 72 hours.

Individual Notification**:** High-risk breaches require direct notification to affected individuals without undue delay.

Documentation**:** All breaches recorded in internal breach log regardless of severity.

Data Sharing and International Transfers

We only share personal data where legally necessary with valid lawful basis. Formal data sharing agreements are established for regular sharing.

The Data Protection Lead maintains a supplier register recording purposes, responsibilities, contracts, retention and data locations. Check processor terms and safeguards for any overseas access or transfer; do not assume all supplier data stays in the UK.

No international transfers occur without adequate protection levels or appropriate safeguards.

Key Retention Periods

- *Foodbank Records***:** 1 year from last service use
- *Debt Advice Files***:** 6 years from case closure
- *Volunteer Records***:** 3 years from end of relationship
- *Employment Records***:** 6 years from employment end
- *Donation Records***:** 3 years from last donation (6 years for Gift Aid)
- *Venue Bookings***:** 3 years from hire date
- *Trustee Minutes***:** Permanent retention

Website Records: Keep minimum payment evidence for six years after the relevant financial year; attendee details for 90 days after the final booked session; expired unpaid bookings for 30 days after expiry; waiting lists for 30 days after the event; resolved enquiries for 12 months; unsuccessful volunteer enquiries for six months after closure.

Routine technical logs: 30 days; access and finance audit logs: 12 months, retaining financial evidence as above. Media permission records: while used and three years afterwards. Backups: expire within 90 days and reapply deletions after recovery. The Data Protection Lead records justified legal or safeguarding holds. Trustees approve these periods; implement and verify deletion before publishing them.

Complaints Process

Under the Data (Use and Access) Act 2025, we handle data protection complaints through a formal process:

1. Complaints accepted in writing to Data Protection Lead
2. Acknowledgement within 30 days
3. Investigation and response without undue delay
4. Right to escalate to ICO if unsatisfied with our response

CCTV Policy (If Implemented)

Any CCTV system requires:

- Formal Board approval with documented legitimate purpose
- Full Data Protection Impact Assessment before installation
- Clear, prominent signage identifying Weston Ark as operator
- Restricted access and maximum 30-day retention
- ICO registration and fee payment

Governance and Responsibilities

Board of Trustees**:** Ultimate legal responsibility for data protection compliance, policy approval, and resource allocation.

Data Protection Lead: Day-to-day compliance oversight, breach management, rights requests, training coordination, ICO liaison.

All Staff and Volunteers**:** Personal responsibility to comply with policy, complete training, handle data securely, report concerns immediately.

Mandatory Training**:** All personnel receive role-specific data protection training during induction and annual refreshers.

Privacy Notice Requirements

All data collection must be accompanied by clear privacy notices explaining:

- Who we are and our Data Protection Lead contact details
- What personal data we collect and why
- Our lawful basis for processing
- Who we share data with and retention periods
- Individual rights and how to exercise them
- How to complain to us and escalate to ICO

Website Notices: Explain booking data, Microsoft services, Stripe and HallMaster. Stripe handles card details; we retain payment references and status. Booking details require a separate lawful basis for marketing. Notices must reflect actual systems and approved retention.

Cookies and Embeds: Record cookies, storage and services including YouTube. Obtain consent unless exempt. Statistical measurement exemptions require clear information and a working objection control, not just browser privacy signals. Review whenever integrations change.

Key Contacts

Data Protection Lead**:** Use the current trustee-confirmed contact register at the Centre for the appointed lead and contact details. **Address:** Hughenden Centre, Weston-super-Mare

Information Commissioner's Office**:**

- Website: www.ico.org.uk
- Helpline: 0303 123 1113
- Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Policy Implementation

This policy is reviewed annually and following significant changes to legislation, technology, or charity operations. All staff and volunteers must comply with these requirements as a condition of their involvement with Weston Ark Charity.

Breach of this policy may result in disciplinary action and could constitute a criminal offence under data protection legislation. The charity takes its legal obligations seriously and expects full cooperation from all personnel in maintaining the highest standards of data protection.

This policy summary contains essential requirements. Full detailed procedures and appendices are available from the Data Protection Lead upon request.

Policy approved by Board of Trustees. Approval confirmed 10 November 2026.