Data Protection Policy

Date: June 2025
Review Date: June 2026

Contents

Appendices

1. Policy Statement

Zest of Mind is committed to protecting the privacy and fundamental rights of all individuals whose personal data we process. We recognise that protecting personal data is not only a legal requirement but also essential for maintaining trust with our community members, volunteers, staff, and stakeholders.

This policy demonstrates our commitment to processing personal data fairly, lawfully, and transparently in accordance with UK GDPR, the Data Protection Act 2018, and other relevant legislation. We are dedicated to implementing appropriate technical and organisational measures to ensure data protection is embedded in all our activities.

Any breach of data protection legislation is considered a serious matter that may result in disciplinary action. All staff, volunteers, trustees, and third parties working with Zest of Mind must comply with this policy.

2. Legal Framework

This policy is based on the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

- The Privacy and Electronic Communications Regulation (PECR)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Electronic Communications (EC Directive) Regulations 2003

3. Definitions

Personal Data: Any information relating to an identified or identifiable living individual.

Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.

Data Controller: The organisation that determines the purposes and means of processing personal data (Zest of Mind).

Data Processor: A third party that processes personal data on behalf of the data controller.

Data Subject: The individual to whom the personal data relates.

Processing: Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.

4. Scope and Application

This policy applies to all personal data processed by Zest of Mind, including:

- Community group members and participants
- Volunteers and volunteer applicants
- Staff and trustees
- Donors and supporters
- Partner organisations and their representatives
- Website visitors and social media followers
- Suppliers and contractors

The policy covers all methods of data processing, whether automated or manual, including paper records, electronic databases, CCTV systems, and communications.

5. Data Protection Principles

We ensure that all personal data is:

5.1 Processed Lawfully, Fairly and Transparently

We ensure that all personal data processing has a clear lawful basis under UK GDPR. We identify and document our lawful basis for each processing activity and provide clear, accessible information about our processing activities to data subjects. We are committed to processing data in ways that individuals would reasonably expect and that do not cause unjustified harm or distress.

5.2 Collected for Specified, Explicit and Legitimate Purposes

We clearly define and communicate why we collect personal data before or at the point of collection. Personal data is only used for the specific purposes outlined at the time of collection or for compatible purposes that are clearly explained to individuals. Any use for new purposes requires establishing an additional lawful basis and providing appropriate notification to affected individuals.

5.3 Adequate, Relevant and Limited

We collect only the personal data that is necessary and proportionate for our specified purposes. Regular reviews are conducted to ensure that data held remains relevant to our charitable objectives and activities. Data that is no longer needed for our purposes is deleted or anonymised in accordance with our retention schedule.

5.4 Accurate and Up-to-Date

We have implemented robust processes to ensure the accuracy of personal data at the point of collection and throughout its lifecycle. We provide accessible mechanisms for individuals to update their information and encourage them to notify us of any changes. Inaccurate or incomplete data is corrected promptly, and we take reasonable steps to verify the accuracy of data we receive from third parties.

5.5 Kept No Longer Than Necessary

We have established clear retention schedules that specify how long different categories of personal data will be kept based on legal requirements, regulatory guidance, and our legitimate business needs. Data is regularly reviewed and securely deleted or anonymised when it is no longer required. We balance our need to retain data for historical, statistical, or legal purposes against individuals' privacy rights.

5.6 Processed Securely

We implement and maintain appropriate technical and organisational security measures to protect personal data against unauthorised access, accidental loss, destruction, or damage. Our security measures are proportionate to the risks posed by our processing activities and the sensitivity of the data involved. All staff receive training on data security procedures and are required to follow our information security policies.

5.7 Accountable

We take responsibility for demonstrating compliance with all data protection principles through comprehensive documentation, regular monitoring, and proactive risk management. We maintain detailed records of our processing activities, conduct regular data protection impact assessments for high-risk processing, and implement privacy by design principles in all our operations.

6. Lawful Basis for Processing

We process personal data under the following lawful bases:

6.1 Legitimate Interests

We rely on legitimate interests as our lawful basis for processing personal data in circumstances where we have a genuine and legitimate reason for doing so, and where our

interests are not overridden by the individual's fundamental rights and freedoms. This includes administering memberships and volunteer programmes, conducting fundraising activities with appropriate safeguards in place, promoting our charitable objectives within our community, and protecting our organisation's legitimate business interests such as preventing fraud or maintaining our reputation.

6.2 Consent

We obtain explicit, freely given consent for processing activities where this is the most appropriate lawful basis. This includes sending marketing communications where these are not covered by our legitimate interests, conducting sensitive fundraising approaches that go beyond normal charitable communications, processing special category data where no other condition applies, and using photographs and video recordings for promotional purposes. Consent can be withdrawn at any time, and we provide clear mechanisms for individuals to do so.

6.3 Legal Obligation

We process personal data where we are required to do so by law. This includes fulfilling our reporting obligations to the Charity Commission, meeting HMRC requirements for Gift Aid and financial reporting, complying with employment law including right to work checks and payroll obligations, and fulfilling our safeguarding duties under relevant child protection and vulnerable adult legislation.

6.4 Vital Interests

We may process personal data without consent where this is necessary to protect someone's life or prevent serious harm. This includes responding to emergency medical situations where immediate action is required, taking action in child protection circumstances where delay could cause harm, and sharing information with relevant authorities to prevent serious criminal activity or threats to public safety.

6.5 Performance of Contract

We process personal data where this is necessary to fulfil our contractual obligations or to take steps before entering into a contract. This includes processing employee data in accordance with employment contracts, managing our relationships with suppliers and service providers in accordance with service agreements, and administering formal volunteer agreements where these constitute contractual relationships.

7. Types of Personal Data We Process

7.1 Standard Personal Data

We process various categories of standard personal data in the course of our charitable activities. This includes contact information such as names, postal addresses, telephone numbers, and email addresses, which we use to communicate with our members, volunteers, and supporters. We also process demographic information including age, gender, and occupation where this is relevant to our services or required for monitoring purposes. Financial information such as donation records and payment details is processed to manage our relationships with supporters and comply with financial regulations. We maintain participation records showing events attended and services used to help us improve our offerings and demonstrate our impact. Communication preferences are

recorded to ensure we contact individuals in their preferred manner and respect their choices about the types of communications they wish to receive. Additionally, we may take and use photographs and video recordings at our events and activities for promotional and record-keeping purposes, always with appropriate consent where required.

7.2 Special Category Data

We recognise that special category data requires enhanced protection and additional safeguards. We only process such data where we have both a lawful basis under Article 6 of UK GDPR and meet one of the conditions for processing under Article 9. Health information may be processed where necessary to make reasonable adjustments for individuals with disabilities, to maintain emergency contact information for safety purposes, or to ensure we can provide appropriate support during our activities. Where our volunteer roles involve working with children or vulnerable adults, we may need to process criminal conviction data as part of our safeguarding procedures, always in proportion to the risks involved and in accordance with relevant guidance. We may collect ethnic origin data on a voluntary basis for equality monitoring purposes to help us ensure our services are accessible to all sections of our community, but this is always optional and individuals can choose not to provide this information without affecting their participation in our activities.

8. Individual Rights

We respect and facilitate the following rights:

8.1 Right to be Informed

- We provide clear privacy information at the point of data collection
- We explain how and why we use personal data
- We detail retention periods and individual rights

8.2 Right of Access

- Individuals can request copies of their personal data
- We respond within one month of receipt
- We provide information free of charge (unless requests are excessive)

8.3 Right to Rectification

- We correct inaccurate or incomplete personal data
- We notify third parties of corrections where appropriate
- We respond within one month

8.4 Right to Erasure ('Right to be Forgotten')

- We delete personal data when it's no longer necessary
- We consider legal requirements and legitimate interests
- We balance deletion requests against our charitable objectives

8.5 Right to Restrict Processing

- We halt processing while investigating disputes
- We maintain minimal records for legal purposes
- We inform individuals before lifting restrictions

8.6 Right to Data Portability

- We provide data in a structured, machine-readable format
- We facilitate direct transfer to other organisations where possible
- This applies to data processed by consent or contract

8.7 Right to Object

- We stop processing for direct marketing upon request
- We consider objections to legitimate interest processing
- We balance individual rights against our charitable purposes

8.8 Rights Related to Automated Decision-Making

- We inform individuals about automated decision-making
- We provide mechanisms to request human intervention
- We allow individuals to challenge decisions

9. Data Retention

We retain personal data only for as long as necessary. Our retention schedule includes:

9.1 Membership and Participation Records

- Active members: Retained whilst membership continues
- Lapsed members: Retained for 2 years after last contact
- Event participants: Retained for 1 year after participation

9.2 Volunteer Records

- Current volunteers: Retained whilst volunteering continues
- Former volunteers: Retained for 6 years after leaving (for reference purposes)
- Unsuccessful applicants: Retained for 1 year

9.3 Employment Records

- Current staff: Retained whilst employment continues
- Former staff: Retained for 6 years after leaving (statutory requirement)
- Recruitment records: Retained for 1 year after appointment

9.4 Financial Records

- Donation records: Retained for 7 years (HMRC requirement)
- Accounting records: Retained for 6 years
- Gift Aid records: Retained for 4 years after claim

9.5 Safeguarding Records

- Retained in accordance with local safeguarding board guidance
- Minimum 25 years or until the individual's 65th birthday (whichever is longer)

9.6 Legal and Governance Records

- Trustee records: Retained permanently
- Legal advice: Retained for 12 years
- Insurance claims: Retained for 12 years

9.7 Data Destruction Process

When personal data reaches the end of its retention period, we ensure secure destruction through the following process:

- **Digital Data**: Securely deleted using data wiping software that overwrites data multiple times, making recovery impossible. Backup copies are also identified and destroyed.
- **Physical Records**: Confidentially shredded using a cross-cut shredder or through a certified document destruction service.
- **Electronic Devices**: Hard drives and storage devices are professionally wiped or physically destroyed before disposal or recycling.
- **Documentation**: All data destruction activities are logged with dates, methods used, and responsible personnel identified.

10. Data Security

We implement appropriate security measures including:

10.1 Technical Measures

- Password protection on all systems (minimum 8 characters, regularly changed)
- Encryption of sensitive data in transit and at rest
- Secure backup procedures with off-site storage
- Firewall protection and anti-virus software
- Regular software updates and security patches
- Multi-factor authentication where available

10.2 Organisational Measures

- Access controls based on job roles and necessity
- Regular staff training on data protection
- Clear desk and clear screen policies
- Secure storage of paper records in locked cabinets
- Controlled access to premises and IT systems
- Regular security audits and risk assessments

10.3 Data Access Controls

Access to different types of personal data is strictly controlled based on job roles and business necessity:

- **All Personal Data**: Only accessible to designated staff members with legitimate business needs
- **Financial Data**: Restricted to treasurer, finance officer, and designated trustees
- **Safeguarding Records**: Accessible only to designated safeguarding officer and relevant senior staff
- **Special Category Data**: Limited to specific roles where processing is necessary and proportionate

- **Volunteer Records**: Accessible to volunteer coordinators and management team
- **Membership Data**: Available to membership coordinators and administrative staff
- **Employment Records**: Restricted to HR personnel and direct line managers

All access is logged and regularly reviewed to ensure ongoing appropriateness.

10.4 Mobile and Remote Working

- Encrypted laptops and mobile devices
- Secure VPN connections for remote access
- Prohibition of storing personal data on personal devices
- Clear policies for working in public spaces

11. Data Sharing and Third Parties

11.1 Internal Sharing

We share personal data internally only:

- On a need-to-know basis
- For legitimate organisational purposes
- With appropriate access controls

11.2 External Sharing

We may share personal data with:

- Other charitable organisations (with appropriate safeguards)
- Professional advisors (solicitors, accountants, consultants)
- Regulatory bodies (Charity Commission, HMRC, ICO)
- IT service providers and data processors
- Emergency services (where necessary)

11.3 Data Processor Agreements

We ensure all data processors:

- Sign comprehensive data processing agreements
- Implement appropriate security measures
- Process data only on our instructions
- Notify us of any data breaches
- Delete data upon contract termination

12. International Transfers

We minimise international transfers of personal data. Where transfers are necessary:

- We ensure the destination country has adequate protection
- We implement appropriate safeguards (Standard Contractual Clauses)
- We conduct transfer impact assessments
- We obtain explicit consent where required

13. Data Breach Management

13.1 Breach Response Team

- Director (or nominated deputy)
- Data Protection Lead
- IT Support (internal or external)
- Legal advisor (if required)

13.2 Breach Response Procedure

1. **Immediate Response (within 24 hours)**
    - Contain the breach and assess ongoing risk
    - Document all known details
    - Notify the breach response team
2. **Assessment (within 72 hours)**
    - Evaluate the severity and impact
    - Determine if ICO notification is required
    - Assess if individuals need to be informed
3. **Notification Requirements**
    - ICO: Within 72 hours for high-risk breaches
    - Individuals: Without undue delay for high-risk breaches
    - Trustees: At next meeting or immediately if severe
4. **Follow-up Actions**
    - Investigate root causes
    - Implement corrective measures
    - Review and update security procedures
    - Provide additional staff training if needed

13.3 Breach Register

We maintain a register of all data breaches, including:

- Date and time of breach
- Nature and cause of breach
- Data and individuals affected
- Actions taken and outcomes
- Lessons learned and improvements made

14. Privacy by Design

We embed data protection considerations into:

- New projects and initiatives from the outset
- System design and procurement decisions
- Policy development and review processes
- Staff recruitment and training programmes
- Partnership agreements and collaborations

15. Staff Training and Responsibilities

15.1 All Staff and Volunteers

- Complete data protection training within first month
- Attend annual refresher training

- Report suspected data breaches immediately
- Follow security procedures and policies
- Seek guidance when uncertain about data protection matters

15.2 Data Protection Lead

- Oversee compliance with this policy
- Conduct regular audits and assessments
- Provide guidance and training to staff
- Act as primary contact for data protection matters
- Monitor changes in legislation and best practice

15.3 Management Team

- Ensure adequate resources for data protection compliance
- Approve significant data protection decisions
- Support the data protection culture
- Report to trustees on compliance matters

16. Monitoring and Review

We monitor compliance through:

- Annual data protection audits
- Regular policy reviews
- Staff feedback and incident reports
- External assessments where appropriate
- Trustee oversight and reporting

This policy is reviewed annually or following:

- Significant changes in legislation
- Major data breaches or incidents
- Organisational restructuring
- Changes in our data processing activities

17. Confidentiality Statement

Zest of Mind is committed to maintaining the highest standards of confidentiality regarding all personal data we process. We recognise that confidentiality is fundamental to data protection and essential for maintaining trust with our community.

Our confidentiality commitments include:

- **Strict Access Controls**: Personal data is only accessible to authorised personnel who require it for legitimate organisational purposes
- **Professional Discretion**: All staff, volunteers, and trustees are bound by confidentiality obligations and must not disclose personal information inappropriately
- **Secure Processing**: All personal data processing activities are conducted with appropriate technical and organisational safeguards to prevent unauthorised access or disclosure
- **Third Party Agreements**: Any external organisations processing data on our behalf are contractually bound to maintain the same standards of confidentiality

- **Training and Awareness**: Regular training ensures all personnel understand their confidentiality obligations and the importance of protecting personal information
- **Incident Response**: Any breach of confidentiality is treated as a serious matter requiring immediate investigation and remedial action

Personal data will only be shared or disclosed where we have a clear lawful basis to do so, typically where required by law, with explicit consent, or where it is in the vital interests of the individual or public safety. In all cases, we ensure that any sharing is proportionate and limited to what is necessary for the specific purpose.

18. Complaints and Contact Information

18.1 Internal Complaints

For questions or concerns about our data protection practices:

Email: admin@zestofmind.com
Phone: 07956 478 393 or 07930 634 523
Address: 56 Guildford Street, Chertsey, England, KT16 9BE

We aim to respond to all enquiries within 10 working days.

18.2 External Complaints

If you remain dissatisfied with our response, you can complain to:

Information Commissioner's Office (ICO)
Website: www.ico.org.uk
Phone: 0303 123 1113
Online: ico.org.uk/make-a-complaint

Our ICO registration number is: ZB733897