St Osyth Priory & Parish Trust

Data Protection Policy

Introduction

St Osyth Priory & Parish Trust is committed to the responsible management, use, and protection of personal data in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and other relevant data protection laws. This Data Protection Policy outlines the Trust's approach to data protection, ensuring that individuals' privacy and rights are respected.

Purpose

To establish the Trust's commitment to data protection and outline the responsibilities and procedures for ensuring compliance with data protection laws, thereby safeguarding personal data against unauthorised access, loss, or disclosure.

Scope

This policy applies to all personal data processed by the Trust, including data held about staff, volunteers, beneficiaries, donors, and any other individuals with whom the Trust interacts. It covers data in both electronic and paper form.

Compliance References

1. **General Data Protection Regulation (UK GDPR)**: Sets out the principles for data processing in the UK.
2. **Data Protection Act 2018**: The UK's implementation of the GDPR.
3. **Electronic Commerce (EC Directive) Regulations 2002:** Covers e-commerce services, such as purchasing tickets for Trust events.
4. **The Privacy and Electronic Communications (EC Directive) Regulations 2003:** sets out protection regarding email marketing, website cookies and tracking, and fundraising communications.

5. **Information Commissioner's Office (ICO) Guidance**: Provides specific guidance on data protection practices.

Principles

The Trust adheres to the following data protection principles:

- **Lawfulness, Fairness, and Transparency**: Personal data will be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation**: Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimisation**: Only data that is necessary for the purposes for which it is processed is collected.
- **Accuracy**: Every reasonable step will be taken to ensure that personal data is accurate and, where necessary, kept up to date.
- **Storage Limitation**: Personal data is kept in a form that permits identification of data subjects for no longer than necessary.
- **Integrity and Confidentiality**: Data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Responsibilities

- **Board of Trustees**: Ensures that the Trust has a comprehensive Data Protection Policy and complies with legal obligations, including appointing a nominated Designated Data Protection Officer [DPO].
- **Governance Committee/Trust Administrator**: Oversees data protection strategy and implementation to ensure compliance with GDPR requirements.
- **All Staff and Volunteers**: Must understand and adhere to this Data Protection Policy and related procedures.

Procedures for Implementation

Data Collection and Consent:

- Clearly communicate the purpose for which data is collected and obtain explicit consent where required.

Data Use and Access:

- Ensure data is only used for the purposes specified and accessed by authorised personnel.

Data Storage and Security:

- Implement appropriate technical and organisational measures to protect data against unauthorised access, alteration, or destruction.

Data Sharing and Transfer:

- Ensure any data sharing or transfers comply with legal requirements, using secure methods and only with parties that also comply with applicable data protection laws.

Rights of Individuals:

- Inform individuals of their rights under GDPR, including access to their data, correction, deletion, and the right to withdraw consent.

Data Breach Response:

- Establish procedures to detect, report, and investigate personal data breaches. Inform the ICO and affected individuals where legally required.

Training and Awareness:

- Provide regular data protection training for staff and volunteers to raise awareness of their responsibilities under GDPR.

Training and Awareness

Ensure that all trustees, staff, and volunteers receive training on Data Protection and Privacy, their roles and responsibilities under this policy.

The Trust is committed to resolving concerns about the use of personal data fairly and promptly.

Any individual who has concerns about how the Trust has collected, used, stored, shared or otherwise processed their personal data may submit a complaint in writing to the Trust's nominated Data Protection Lead.

The Trust will:

• Acknowledge receipt of the complaint within 30 calendar days.

• Investigate the matters raised and make appropriate enquiries.

• Keep the complainant informed of progress where an investigation is ongoing.

• Communicate the outcome of the investigation, including any action taken by the Trust.

• Inform the complainant of their right to escalate the matter to the Information Commissioner's Office (ICO) if they remain dissatisfied.

In addition to complaints, individuals have the right to confirm whether their personal data is being processed and to request a copy of that information (Subject Access Request [SARs]).

Requests may be made in writing or electronically and should be directed to the Trust's nominated Data Protection Lead.

Upon receipt of a Subject Access Request, the Trust will:

• Verify the identity of the requester where necessary.

• Record the request and relevant deadlines.

• Conduct reasonable and proportionate searches for personal data held by the Trust.

• Consider whether any exemptions apply under data protection legislation.

• Respond without undue delay and normally within one calendar month.

• Maintain appropriate records of requests and responses.

Where information is withheld under a statutory exemption, the Trust will explain the basis for that decision unless prevented from doing so by law.

Individuals dissatisfied with the Trust's response may raise a complaint through the Trust's Data Protection Complaints Procedure and may also complain to the Information Commissioner's Office (ICO).

Policy Review

This policy will be reviewed annually at the Trust' AGM or as needed to ensure compliance with new or revised data protection laws, guidance from the ICO, or changes in the Trust's operations. Amendments will be approved by the Board of Trustees.

APPROVED:

DATE:

REVIEW & REVISION: