Policy on Data Protection

Parish of Holy Trinity with St Columba, Fareham

This Policy explains how the Parish of Holy Trinity with St Columba, Fareham (HTSCF) will comply with its responsibilities and obligations under the Data Protection Act 2018. These laws regulate the 'processing' of personal data to protect the rights of individuals, by placing responsibilities and obligations on HTSCF and its staff.

Policy Objectives

- To ensure personal data is processed by HTSCF in a consistent manner and in accordance with the DPA & GDPR.
- To set out HTSCF's approach to data protection.
- To clarify the responsibilities within HTSCF for implementing the policy and monitoring compliance.
- To ensure that staff work in accordance with HTSCF's information compliance policies.
- To provide guidance to staff to minimise the risk of unauthorised or unlawful access or use of personal data and against accidental loss or destruction of, or damage to, personal data.

Policy Scope

HTSCF's Data Protection Policy shall include the following:

- All personal data for which HTSCF is responsible including information assets held, processed or stored on HTSCF premises or at approved off-site premises.
- All supporting assets (for example premises, IT systems and networks) upon which the security of personal data depends.

This Policy shall apply to all HTSCF employees, whether full-time, part-time, permanent, temporary or casual. It shall also apply to any contractors or third party users who have authorised access to any HTSCF personal data.

This policy applies to personal data held by HTSCF in all formats, including manual records/paper files and on computers, (e.g. desktops, laptops, tablets, iPads and smartphones).

Policy Statements

Definitions

'Staff' includes anyone working for HTSCF including employees, volunteers, work experience candidates, committee members and any other person with authorised access to personal data held by HTSCF, e.g. consultants and contractors.

'Personal data' means information about a living individual who can be identified from that data. NB: This includes any expression of opinion about an individual.

Examples of personal data typically processed by HTSCF are:

- Names, Postal and email addresses, Home Telephone numbers, Bank account details, Personnel records including medical details, Staff personal reviews

'Sensitive personal data' means personal data about:

- Racial or ethnic origin, political opinions, religious and other beliefs, Trade union membership, physical or mental health, sex life, legal proceedings about an offence.

Sensitive personal data must be treated with greater care than other personal data. This means that such data has to be the subject of additional, stringent, conditions in order to be fairly processed.

Staff who are unsure when sensitive personal data should be processed should seek advice from the incumbent.

'Processing' includes obtaining, recording, holding, using, filing, organising, transmitting, retrieving, disseminating, sharing (disclosing), destroying, adapting, retrieving, erasing and storing personal data. This means that virtually anything HTSCF does with personal data will be processing.

A 'data subject' is any living individual whose personal data is processed by HTSCF e.g. staff, volunteers, members of the electoral roll, congregation members and general public.

The principles of data protection

The DPA requires that HTSCF must comply with eight data protection principles. These principles mean that personal data must:

- Be fairly and lawfully processed: Nobody should be deceived or misled about the purpose for which their data is to be processed.
- Be processed for limited purposes: Personal data can only be obtained for specified and lawful purposes with permission from the data subject for each purpose.
- Be adequate, relevant and not excessive: The personal data must be sufficient to meet the purpose(s) it has been obtained for, but not provide more information than is required, or that is outside the scope of the purpose(s).
- Be accurate: The personal data must be accurate when recorded and accuracy must be maintained throughout the lifecycle of the data.
- Not be kept for longer than is necessary: Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained.
- Be processed in line with the rights of the data subject: Data subjects have rights, including the right to access their personal data.
- Be stored and processed securely: All appropriate measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction.
- Not be transferred to other countries without adequate protection: Personal data must not be transferred to a country outside the European Economic Area unless that country has in place a level of data protection comparable to that in the EU.

Rights of Data Subjects

All data subjects of HTSCF have the following rights under the DPA:

- A right of access to a copy of the information comprised in their personal data (see below)
- A right to object to processing that is likely to cause or is causing damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed and

- A right to claim compensation for damages caused by a breach of the DPA

These rights are extended under GDPR to:

- An enhanced right to information and transparency
- A right of access and rectification
- A right to erasure or "right to be forgotten"
- A right to restriction
- A right to data portability

Subject Access Requests

Any data subject who wants to exercise their right of access to a copy of the information comprised in their personal data, can do so by making a Subject Access Request ('SAR'). This would normally be through the Parish Office but is equally valid if submitted to any member of the HTSCF staff.

A SAR must normally be made in writing and answered within 40 calendar days of receipt.

Any member of staff in receipt of a SAR must pass it on to the Parish Office as soon as possible and in any event within 24 hours.

Collecting and using personal data

HTSCF typically collects and uses personal data in support of its work as a Parish.

HTSCF collects personal data mainly in the following ways:

- By asking contacts to complete paper forms.
- By asking contacts to complete online forms
- By asking contacts to give information verbally or by telephone.

HTSCF will:

- Not use any of the personal data it collects in ways that have unjustified adverse effects on the individuals concerned
- Be transparent about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data
- Handle people's personal data only in ways they would reasonably expect and
- Not do anything unlawful with the data.

Disclosing (sharing) personal data

This includes the disclosure (sharing) of personal data both to another organisation AND the sharing of personal data of data subjects between staff in the parish.

HTSCF will not disclose personal data to another organisation unless the data subject has given consent, or as otherwise permitted by the DPA.

Staff of HTSCF must not disclose personal data of data subjects to one another unless the data subject has given consent or the disclosure has been authorised.

Keeping Data Secure

HTSCF will take all appropriate measures to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction.

GDPR requires that we have demonstrable measures to protect the personal data that we hold. We will protect the personal data using a risk-based Information Security Management System as set out in our Information Security Policy.

Retention of personal data

HTSCF will not keep personal data for longer than is necessary.

Disposal of personal data

When it is no longer necessary to keep it, personal data will be deleted or disposed of securely. This means that:

- Paper personal data will be shredded on site, or disposed of externally as confidential waste.
- Electronic media will be disposed of securely.
- Computer equipment that is surplus to requirements will be disposed of securely.
- A register will be maintained to record details of the media and computer equipment that has been disposed of, when it was disposed, how it was disposed and by whom.

Transfer of personal data outside EEA

Personal data will not be transferred to a country outside the European Economic Area unless HTSCF is satisfied that a level of data protection is in place that is comparable to that required in the EU.

Responsibilities

The PCC have ultimate responsibility for ensuring HTSCF complies with the DPA and the data protection principles. The PCC and Rector together are the Data Controller for the Parish.

The Data Compliance Officer has day-to-day operational responsibility for ensuring HTSCF complies with the DPA and the data protection principles.

In addition, all staff have a responsibility to comply with the DPA and the data protection principles and are responsible for ensuring that they work securely and in accordance with this policy.

Line Managers are responsible for supporting their staff's adherence with this policy.

Documentation

The GDPR requires that the Parish documents what personal data is held, how it is processed and how it is secured. This documentation will be maintained by the Data Compliance Officer and retained in the Parish Office.

Document Control

This Policy needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in activities, which will or could possibly affect the current operation of the Parish Information Security Management System, and the relevance of this document
- A change in the manner in which the Parish manages or operates its information assets and/or their supporting assets, which may affect the accuracy of this document
- An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident, formal review or an audit finding.

Agreed and paper copy signed August 2021