St Michael's Fellowship Data Protection Policy

Updated:	October 2022

1. Personal data

This Policy applies to all 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (including name, identification number, location data or online identifier).

This applies to both automated personal data and manual filing systems where personal data are accessible according to specific criteria. Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include race/ethnicity, physical and mental health, sexual life, offences/ alleged offences, plus genetic/biometric data where processed to uniquely identify an individual.

2. Data Protection Principles

St Michael's is committed to processing data in accordance with its responsibilities under GDPR, which requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

St Michael's recognises the Individual Rights as set out under GDPR (noting that these rights do not apply in all circumstances):

1. *The right to be informed*
2. *The right of access*
3. *The right to rectification*
4. *The right to erase*
5. *The right to restrict processing*
6. *The right to data portability*
7. *The right to object*
8. *Rights in relation to automated decision making and profiling*

3. General Provisions

a) This policy applies to all personal data and sensitive personal data processed by St Michael's
b) The Responsible Person (the Director) is responsible for St Michael's ongoing compliance with this policy
c) This policy provides comprehensive but proportionate measures in line with ICO guidelines
d) This policy will be reviewed annually
e) St Michael's is registered with the Information Commissioner's Office (ICO) as an organisation that processes personal data

4. Lawful, fair and transparent processing

a) To ensure its processing of data is lawful, fair and transparent, St Michael's maintains a Register of Systems and records the lawful basis for each identified data group
b) The Register is reviewed at least annually
c) Individuals have the right to access their personal data and any such request made to St Michael's will be dealt with in a timely manner (maximum 30 days)

5. Lawful purposes processing data

All data processed by St Michael's is on one of the following lawful bases, and the appropriate lawful basis is recorded within the Register of Systems:

a) - Consent of the data subject

b) - Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

c) - Processing is necessary for compliance with a legal obligation

d) - Processing is necessary to protect the vital interests of a data subject or another person

e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Where consent is relied upon as a lawful basis for processing data, St Michael's requires a positive opt-in and evidence of the consent is held with the personal data.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent is clearly available, and systems have been put in place to ensure that such revocation is reflected timely and accurately in St Michael's systems.

6. Privacy Policy

a) St Michael's has provided a privacy policy to each identified data group

7. Data accuracy and minimisation

a) St Michael's takes reasonable steps to ensure personal data is accurate
b) Where necessary for the lawful basis on which data is processed, steps are in place to ensure personal data is kept up to date
c) St Michael's is committed to ensuring that personal data held is adequate, relevant and limited to what is necessary to the purpose for which it is processed
d) To ensure that data is kept for no longer than necessary, St Michael's has identified the legal requirements for retaining data (for how long and why) for each identified data group
e) St Michael's has a system in place for deleting personal data at an individual's request where there is no ongoing legal obligation to retain the data

8. **Security**

a) St Michael's has put IT systems in place to ensure that personal data held electronically is stored securely using modern software that is kept up to date
b) St Michael's has suitable and restricted filing systems for secure storage of paper records
c) Access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information
d) When personal data is deleted this is done safely such that the data is not recoverable
e) Appropriate back-up and disaster recovery solutions are in place
f) St Michael's does not transfer any personal data outside the European Union or to international agencies

9. **Breaches**

a) In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, St Michael's will promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO
b) St Michael's will also assess the risk to the reputation or financial stability of the charity and if appropriate report this to the Charity Commission

Appendices

1. Register of Systems and the lawful basis of processing for each identified data group
2. Privacy notices for each group (Residential Assessment, Contact Centre, Supporters, Outreach, Securing Change, Caring Dads)
3. Consent for each group (within Residential Placement Agreement, Outreach Assessment, Contact Working Agreement, Employee Details form)
4. Direct marketing strategy
5. Cookies policy
6. Subject Access Request policy – Individual's Rights
7. Data breach policy
8. Use of mobile devices for monitoring and recording, and deletion of data on completion
9. Archiving and deletion processes
10. IT and Information Security policy (covers document management, general IT security, virus protection and Firewall policy, authorised software list)
11. Register of data processors
12. New business case template

Explanatory Notes: Detail of Individual Rights under GDPR

1. Right to be informed

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data. Should be concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge

2. Right of access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing
You must provide a copy of the information free of charge**,** without delay and within one month

3. Right to rectification

The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete. You must respond within one month

4. Right to erasure

The right to erasure is also known as 'the right to be forgotten'. Individual can request deletion or removal of personal data where there is no compelling reason for its continued processing
You can refuse to comply with a request for erasure where the personal data is processed for specified reasons (eg legal obligation or official authority)

5. Right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data.
When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information to ensure restriction is respected in future.
(eg where individual contests accuracy of personal data, restrict processing until verified)

6. Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way (eg to take advantage of services which use data to find a better deal, or help understand spending habits)
You must provide personal data in structured, commonly used, machine readable form (eg CSV)

7. Right to object

Individuals have the right to object to processing of personal data
You must stop processing the personal data unless: you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

8. Rights related to automated decision making including profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with requirements of the GDPR.