HIGHAM WITH MERSTON PAROCHIAL CHURCH COUNCIL

GDPR and Data Protection Policy

For the purposes of this policy the meaning of the words is to be those ascribed to them in the glossary below.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the Processing of Personal Data relating to them.

Data Compliance Officer means a natural or legal person appointed for and on behalf of the Data Controller (Incumbent and/or PCC) to ensure adherence to the GDPR at St John's Church, Higham.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The Incumbent and/or the PCC are the Data Controllers of all Personal Data relating to Data Subjects.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data Processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the Processing of Personal Data.

Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of and with authority from the Data Controller.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data is any information relating to an identified or identifiable natural person (Data Subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when information is collected about them. These notices may take the form of general privacy statements applicable to a specific group of individuals or they may be stand-alone privacy statements covering Processing related to a specific purpose.

Processing means anything done with Personal Data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's Personal Data.

This policy is intended to ensure that Personal Data is dealt with properly and securely and in accordance with the legislation. It will apply to Personal Data regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

The Data Controller will comply with their obligations under the GDPR and DPA. They are committed to being concise, clear and transparent about how they obtain and use Personal Data and will ensure Data Subjects are aware of their rights under the legislation.

All Processors must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All Processors must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the Data Controller, and all Processors comply with the legislation.

Scope of the Policy

Personal Data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR Personal Data also includes an identifier such as a name, an identification number, location data or an online identifier.

The Data Controller collects Personal Data for the effective functioning of St John's Church, Higham. In addition, it may be required by law to collect and use certain types of Personal Data to comply with statutory obligations.

[1] GDPR Article 4 Definitions

The Principles
The principles set out in the GDPR must be adhered to when Processing Personal Data:

1. Personal Data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**);
2. Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**);
3. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**);
4. Personal Data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that Personal Data that are inaccurate are erased or rectified without delay (**accuracy**);
5. Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose for which the Personal Data is processed (**storage limitation**); and
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the Data Subject and to ensure that Personal Data is processed in a manner that ensures appropriate security of the Personal Data and protects against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data (**integrity and confidentiality**).

Transfer Limitation

In addition, Personal Data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[2].

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the Data Subject has provided explicit Consent or for other limited reasons.

[2] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

Lawful Basis for Processing Personal Data

Before any Processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the Processing activity and the most appropriate lawful basis (or bases) for that Processing must be selected from the following:

- 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 Data Controller;
- Processing is necessary for the performance of a contract to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party[3]; and
- The Data Subject has given Consent to the Processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, the Consent form must be kept separate from those other matters.

  Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if Personal Data is intended to be processed for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the Processing and the lawful basis or bases for it in the PCC's relevant Privacy Notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful Processing (only where appropriate outside the Data Controller's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a DPIA may also need to be conducted.

[3] The GDPR states that legitimate interests do not apply to Processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

Sensitive Personal Data

Processing of Sensitive Personal Data (known as 'special categories of Personal Data') is prohibited[4] unless a lawful special condition for Processing is identified.

Sensitive Personal Data will only be processed if:

- There is a lawful basis for doing so as identified on previous page and
- One of the special conditions for Processing Sensitive Personal Data applies:
    - (a) the Data Subject has given explicit Consent (which has been clearly explained in a Privacy Notice);
    - (b) the Processing is necessary for the purposes of exercising the employment law rights or obligations of the Data Controller or the Data Subject;
    - (c) the Processing is necessary to protect the Data Subject's vital interests, and the Data Subject is physically incapable of giving Consent ;
    - (d) the Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim;
    - (e) the Processing relates to Personal Data which are manifestly made public by the Data Subject;
    - (f) the Processing is necessary for the establishment, exercise or defence of legal claims;
    - (g) the Processing is necessary for reasons of substantial public interest;
    - (h) the Processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services; or
    - (i) the Processing is necessary for reasons of public interest in the area of public health.

The Privacy Notice(s) set out the types of Sensitive Personal Data processed, what it is used for, the lawful basis for the Processing and the special condition that applies.

Sensitive Personal Data will not be processed until an assessment has been made of the proposed Processing as to whether it complies with the criteria above and the individual has been informed (by way of a Privacy Notice or Consent) of the nature of the Processing, the purposes for which it is being carried out and the legal basis for it.

Unless the Data Controller can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Evidence of Consent will need to be captured and recorded so that compliance with the GDPR can be demonstrated.

[4] GDPR, Article 9

Data Protection Impact Assessments (DPIA)
All Data Controllers are required to implement 'Privacy by Design' when Processing Personal Data.

This means the PCC's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like Pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where Processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the Processing is necessary and proportionate in relation to its purpose;
- the risks to Data Subjects; and
- what measures can be put in place to address those risks and protect Personal Data.

Documentation and records

Written records of Processing activities must be kept and recorded including:

- the name(s) and details of Data Subjects or roles that carry out the Processing;
- the purposes of the Processing;
- a description of the categories of Data Subjects and categories of Personal Data;
- categories of recipients of Personal Data;
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- retention schedules; and
- a description of technical and organisational security measures.

As part of the PCC's record of Processing activities the Data Compliance Officer will document, the following:

- information required for Privacy Notices;
- records of Consent ;
- controller-processor contracts;
- the location of Personal Data;
- DPIAs; and
- Records of Data Breaches.

Records of Processing of Sensitive Data are kept on:

- The relevant purposes for which the Processing takes place, including why it is necessary for that purpose;
- The lawful basis for our Processing; and
- Whether the Personal Data is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

Privacy Notice

The Data Controller will issue Privacy Notices as required, informing Data Subjects (or their parents, depending on age of the child) about the Personal Data that it collects and holds relating to individual Data Subjects, how individuals can expect their Personal Data to be used and for what purposes.

When Personal Data is collected directly from Data Subjects, the Data Subject shall be given all the information required by the GDPR including the identity of the Data Controller, how and why the Data Controller will use, process, disclose, protect and retain that Personal Data through a Privacy Notice.

When Personal Data is collected indirectly (for example from a third party or publicly available source) the Data Subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the Personal Data. The Data Controller must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed Processing of the Personal Data.

The Data Controller will take appropriate measures to provide information in Privacy Notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The Data Controller will issue a minimum of two Privacy Notices, one for role holder information, and one general notice, and these will be reviewed in line with any statutory changes.

Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal Data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and they have consented where necessary.

Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Processors may only process data when their role requires it and must not process Personal Data for any reason unrelated to their role.

The Data Controller will ensure Personal Data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Processors must take all reasonable steps to destroy or delete all Personal Data that is held in their systems when it is no longer required. This includes requiring third parties to delete such data where applicable.

The Data Controller must ensure that Data Subjects are informed of the period for which Personal Data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights
All Data Subjects have the following rights in relation to their Personal Data:

- To be informed about how, why and on what basis that information is processed *(see the relevant Privacy Notice);*

- To obtain confirmation that Personal Data is being processed and to obtain access to it and certain other information, by making a subject access request *;*

- To have data corrected if it is inaccurate or incomplete;

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the Processing ('the right to be forgotten');

- To restrict the Processing of Personal Data where the accuracy of the information is contested, or the Processing is unlawful (but you do not want the data to be erased) or where the Data Controller no longer needs the Personal Data, but you require the Personal Data to establish, exercise or defend a legal claim;

- To restrict the Processing of Personal Data temporarily where you do not think it is accurate (and the Data Controller is verifying whether it is accurate), or where you have objected to the Processing (and they are considering whether their legitimate grounds override your interests);

- In limited circumstances to receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format;

- To withdraw Consent to Processing at any time (if applicable);

- To request a copy of an agreement under which Personal Data is transferred outside of the EEA;

- To object to decisions based solely on Automated Processing, including profiling;

- To be notified of a Personal Data Breach which is likely to result in high risk to their rights and obligations; and

- To make a complaint to the ICO or a Court.

Individual Responsibilities
The Data Controller and Data Processors may have access to the Personal Data of other Data Subjects. The Data Controller expects Data Processors to help meet its data protection obligations to those individuals.

If you have access to Personal Data, you must:

- only access the Personal Data that you have authority to access and only for authorised purposes;
- only allow other Data Processors to access Personal Data if they have appropriate authorisation;
- only allow individuals to access Personal Data if you have specific authority to do so;
- keep Personal Data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the PCC's policies); and
- not remove Personal Data, or devices containing Personal Data (or which can be used to access it) from the church premises unless appropriate security measures are in place (such as Pseudonymisation, encryption or password protection) to secure the data and the device.

Information Security
The Data Controller will use appropriate technical and organisational measures to keep Personal Data secure, to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

Processors are responsible for keeping information secure in accordance with GDPR and other relevant legislation and must follow this policy.

The Data Controller will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of Personal Data that it owns or maintains on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). It will evaluate and test the effectiveness of those safeguards to ensure security of Processing, as circumstances require.

Processors must guard against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. They must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

Processors must follow all procedures and technologies put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. They may only transfer Personal Data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Processors must maintain data security by protecting the **confidentiality, integrity and availability** of the Personal Data, defined as follows:

> **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it.
>
> **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed.
>
> **Availability** means that authorised users can access the Personal Data when they need it for authorised purposes.

Where the Data Controller uses external organisations to process Personal Data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of Personal Data. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the Data Controller;
- Processors are subject to the duty of confidence;
- appropriate measures are taken to ensure the security of Processing;
- sub-contractors are only engaged with the prior Consent of the Data Controller and under a written contract;
- the organisation will assist the Data Controller in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will delete or return all Personal Data to the Data Controller as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the Data Controller with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell them immediately if it does something infringing data protection law.

Storage and retention of Personal Data
Personal Data must be kept securely in accordance with data protection obligations.

Personal Data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why Personal Data was obtained.

Personal Data Breaches
A Personal Data Breach may take many different forms including, but not limited to:

- Loss or theft of data or equipment on which Personal Data is stored;
- Unauthorised access to or use of Personal Data;
- Loss of data resulting from an equipment or systems (including hardware or software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- Blagging offences where information is obtained by deceiving the organisation which holds it.

The Data Controller must report a Personal Data Breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of Data Subjects. The Data Controller must also notify the affected Data Subjects if the breach is likely to result in a high risk to their rights and freedoms.

Processors should ensure they inform the Data Controller or the Data Compliance Officer immediately that a Personal Data Breach is discovered and make all reasonable efforts to recover the Personal Data.

Training
The Data Controller will ensure that Processors are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply
The Data Controller takes compliance with this policy very seriously. Failure to comply puts Data Subjects whose Personal Data is being Processed at risk and carries the risk of significant civil and criminal sanctions for the Processor, and the Data Controller and may in some circumstances amount to a criminal offence by the Processor.

If a Processor breaches this policy, then authority to Process Personal Data for and on behalf of the Data Controller may be terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact the Data Controller or the Data Compliance Officer.

Review of Policy
This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Supervisory Authority in the UK
Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, Personal Data Breaches, dealing with subject access requests, how to handle requests from third parties for Personal Data etc. July 2018