**Kingston Greek Orthodox Community of**

**St George the Great Martyr**

**DATA PROTECTION POLICY**

**Introduction**

*Purpose*

Our community is committed to being transparent about how it collects and uses the personal data of its workforce, members, and to meeting its data protection obligations. This policy sets out the community’s commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of all current and past workers, contractors and volunteers.

The community has appointed Mr. Panayiotis Toumazi and Mr. Ioannis Mansolas as its data protection officers. Their role is to inform and advise the community on its data protection obligations. They can be contacted at ptoumazi@aol.com and ioannis.mansolas@btinternet.com. Questions about this policy, or requests for further information, should be directed to the data protection officers.

*Definitions*

**"Personal data"** is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**Data protection principles**

The community processes HR-related personal data and personal data of members, volunteers and employees, in accordance with the following data protection principles:

* The community processes personal data lawfully, fairly and in a transparent manner.
* The community collects personal data only for specified, explicit and legitimate purposes.
* The community processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
* The community keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
* The community keeps personal data only for the period necessary for processing.
* The community adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The community will not process personal data of individuals for other reasons. Where the community relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the community processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The Community will update HR-related personal data and personal data of parents, guardians and students promptly if an individual, parent or guardian advises that his/her information has changed or is inaccurate.

Personal data gathered during the [employment, worker, contractor or volunteer relationship, or apprenticeship or internship] is held in the individual's personnel file (in hard copy or electronic format, or both), and on electronic systems. The periods for which the Community keeps HR-related personal data and personal data of parents, guardians’ students and community members are contained in its privacy notices to individuals.

The Community keeps a record of its processing activities in respect of HR-related personal data and personal data of members, employees and volunteers, in accordance with the requirements of the General Data Protection Regulation (GDPR).

**Individual rights**

As a data subject, individuals have a number of rights in relation to their personal data.

*Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Community will tell him/her:

* whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
* to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
* for how long his/her personal data is stored (or how that period is decided);
* his/her rights to rectification or erasure of data, or to restrict or object to processing;
* his/her right to complain to the Information Commissioner if he/she thinks the Community has failed to comply with his/her data protection rights; and
* whether or not the Community carries out automated decision-making and the logic involved in any such decision-making.

The Community will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the Community will charge a fee, which will be based on the administrative cost to the Community of providing the additional copies.

To make a subject access request, the individual should send the request to ptoumazi@aol.com or ioannis.mansolas@btinternet.com. In some cases, the Community may need to ask for proof of identification before the request can be processed. The Community will inform the individual if it needs to verify his/her identity and the documents it requires.

The Community will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Community processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Community will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Community is not obliged to comply with it. Alternatively, the Community can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Community has already responded. If an individual submits a request that is unfounded or excessive, the Community will notify him/her that this is the case and whether it will respond to it or not.

*Other rights*

Individuals have several other rights in relation to their personal data. They can require the Community to:

* rectify inaccurate data;
* stop processing or erase data that is no longer necessary for the purposes of processing;
* stop processing or erase data if the individual's interests override the community's legitimate grounds for processing data (where the Community relies on its legitimate interests as a reason for processing data);
* stop processing or erase data if processing is unlawful; and
* stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the community's legitimate grounds for processing data.

To ask the Community to take any of these steps, the individual should send the request to ptoumazi@aol.com or ioannis.mansolas@btinternet.com

**Data security**

The Community takes the security of HR-related personal data and personal data of members, employees and volunteers seriously. The Community has internal controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Community engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

**Data breaches**

If the Community discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Community will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**International data transfers**

The Community will not transfer personal data to countries outside the EEA.

**Individual responsibilities**

Individuals are responsible for helping the Community keep their personal data up to date. Individuals should let the Community know if data provided to the Community changes, for example if an individual move to a new house.

Individuals may have access to the personal data of other individuals during their employment, contract, or volunteer period. Where this is the case, the Community relies on individuals to help meet its data protection obligations to staff, parents and students.

Individuals who have access to personal data are required:

* to access only data that they have authority to access and only for authorised purposes;
* not to disclose data except to individuals (whether inside or outside the Community) who have appropriate authorisation;
* to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
* not to remove personal data, or devices containing or that can be used to access personal data, from the Community’s premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
* not to store personal data on local drives or on personal devices that are used for work purposes; and
* to report data breaches of which they become aware to the data protection officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Community’s disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

**Training**

The Community will provide training to all individuals about their data protection responsibilities as part of the induction process, and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

**CONSENT LETTER**

**Name(s) of Community member(s):……………………………………………………….**

Dear member,

You are probably aware of the new General Data Protection Regulation (GDPR) designed to strengthen and unify the safety and security of all data held within an organisation. At St George’s community, we are rightly expected to adhere to this.

At the community, we need to use and store information about you. This information is used to share community information and activities.

In order to comply with laws regarding data sharing we would like your consent in order to do this and to use the information in the ways described above. If you require further information, please refer to the General Data Protection Regulation Information on <https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>

If you are not happy to share the information as described above, please let us know so that your preferences, where possible, can be accommodated.

We really value having access to your personal data as it supports the effective and smooth running of the community.

Please tick the relevant box below to indicate your preference and return this form to the community Data Protection Officers Mr Panayiotis Toumazis and/or Mr Ioannis Mansolas at your earliest convenience.

**I agree for the community to use the data to communicate with me for any community related issues.**

OR

I do **NOT** agree for the community to use my data for any of the above purposes (ticking this box will mean you will not receive community communications, letters or any other correspondence from the community)

If you change your mind at any time, you can let us know by emailing the community office at **info@stgeorgecommunity.co.uk** or by simply popping to the community office at Pangari at the Church to discuss.If you have any other questions, please get in touch.

DECLARATION

Name :………………………………………………………………….

Signed: …………………………………………………………………..

Date: …………………………………………………

 EMAIL:……………………………………………………………………………………………… TELEPHONE:………………………………