Greek Orthodox Church
of Saint Peter & Saint Paul in Bristol

Data Protection Policy

Introduction

The Data Protection Act 2018 (DPA 18) and the General Data Protection Regulation (GDPR) commenced on 25th May 2018.

GDPR regulates the "processing" of personal information and includes obtaining, storing, viewing, using, updating, disclosing and destroying any data held electronically, in structured manual records and to a limited extent to unstructured manual records.

Personal data within DPA 18 and GDPR covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

The Greek Orthodox Church of Saint Peter and Saint Paul in Bristol (Greek Orthodox Church) is committed to:

- using personal data lawfully, fairly and in a transparent way
- collecting relevant personal data only for valid purposes that are clearly explained
- keeping accurate and up to date personal data
- only keeping personal data only as long as necessary for the purposes that have been defined
- kept securely

The Organisation privacy notice(s) describe how we collect and use personal information about employees, contractors, volunteers and service users in accordance with GDPR.

This policy outlines the responsibilities with regard to the Data Protection Act 2018 and the General Data Protection Regulation, of all staff (including 3rd parties under contract), volunteers. Senior Parish and committee members.

All are required to handle and process data (records or systems) in accordance with this policy and in accordance with other related policies concerning the handling or processing of data.

Employee Responsibilities:

- familiarise yourself with this policy and other information made known to you by the Organisation
- comply with all aspects of this policy and other information made known to you by the Organisation
- report any potential breaches in data protection at the earliest opportunity
- actively participate in data protection training provided by the Greek Orthodox Church
- on receipt of a request from an individual for information held, known as subject access requests or concerns about processing of personal information, immediately notify Andreas Nicolaou, Treasurer, responsible for Data Protection at Greek Orthodox Church
- follow the subject access request procedure
- actively seek clarification from Andreas Nicolaou on any questions or queries you have on this policy, Greek Orthodox Church privacy notices or data protection in general

Greek Orthodox Church Responsibilities:

- ensure any personal data is collected in a fair and lawful way
- explain at the outset why information is being collected, what it will be used for and with whom it will be shared
- ensure any new or planned projects that involve personal data are preceded with a data privacy impact assessment.
- ensure that access controls are limited to role relevance
- gain explicit consent where required
- ensure that only the minimum amount of information needed is collected and used
- ensure the information used is up to date and accurate
- review the length of time information is held in line with relevant legislation
- ensure information is kept safely
- ensure the rights people have in relation to their personal data can be exercised
- dispose of data appropriate and without unnecessary delay
- ensure that anyone managing and handling personal information is trained to do so
- ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, senior member or volunteer knows what to do
- any disclosure of personal data will be in line with relevant legislation, and internal policies and procedures
- any sharing of data to third parties is covered by a data sharing agreement
- take measures to ensure safe transfers of data outside of the EU/EEU where cross border sharing is necessary

Data Security:

All staff, senior members and volunteers of the Greek Orthodox Church must ensure personal information is protected from unauthorised viewing and from loss (including computer documents, emails and paper copies. Staff and senior members will be provided with adequate awareness training and must follow guidelines provided by the organisation as set out in the GDPR code of practice:

- use lockable cupboards (restricted access to keys)
- mandatory renewal of passwords to agreed frequency
- password protect personal information files
- setting up computer systems to allow restricted access to certain areas
- not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) without adequate safeguarding i.e. encryption
- if personal data can be taken off site, in which forms (paper, memory stick, and laptop), instructions will be given to the staff member, senior member of the church or volunteer about keeping it safe
- secure and reliable security back up of data
- password protected attachments for sensitive personal information sent by email
- robust and trustworthy IT security features
- secure data flows across organisation and 3rd party data sharing requirements
- robust secure on-site IT storage facility of electronic data
- ensure all disposals of data are correctly destroyed using accredited organisations and appropriate certification is obtained
- ensure the use of confidential waste receptacles
- ensure data is not shared without the explicit consent of the subject, where no exemptions apply
- set adequate access controls which role specific
- take measures to ensure safe transfers of data outside of the EU/EEU where cross border sharing is necessary
- continuous review of all measures

The Greek Orthodox Church will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. All staff, senior members or volunteers must take reasonable responsibility to ensure the data is accurate and up to date, relevant and not excessive.

Any unauthorised disclosure of personal data to a third party by any staff, senior members or volunteers of the Greek Orthodox Church may result in disciplinary or legal action. Failure to comply with the organisations policies and procedures for handling personal data is a disciplinary offence which may be considered gross misconduct and may also involve personal criminal liability.

Data subject rights

Anyone whose personal information the Greek Orthodox Church processes has the right to know:

- what information the organisation holds and processes about them
- the legitimate reasons for processing
- the right to consent or withdraw consent
- how to gain access to this information
- how to keep it up to date
- to receive this data in a clear format
- to receive this data within one month
- data subjects have the right to prevent processing of their personal data in some circumstances and have the right to correct, rectify, block or erase information regarded as incorrect
- to be informed of any miss-use or loss of this data if the loss represents a high risk to the rights and freedoms of individuals
- the right to erasure of personal information – commonly referred to as the right to be forgotten
- the right to complain and/or seek compensation

Individuals have a right under the Regulation to ask the Greek Orthodox Church if it holds their personal data, and if so, be provided with a copy of it, this is known as subject access requests.

Subject Access Requests (SAR)

Any person wishing to exercise this right should apply in writing to Andreas Nicolaou, Treasurer. The following information will be required before access is granted:

- full name
- date of birth
- national insurance number

Proof identity may be required. The following forms of ID will be acceptable:

- birth certificate
- passport
- driving licence

SAR's will be dealt with in line with the GDPR recommended timescales. The organisation will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within one month as required by the Regulation from receiving the written request.

Where requests are numerous and/or complex this may be extended by two further months. Where an extension is applied the requester will be advised within the one month including the reason why the additional time is needed.

SAR's will normally be processed free of charge, where the organisation deems the request to be unfounded or excessive; if it is repetitive, or if the same information is requested. Then the

organisation may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility.

The organisation is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

In principle, the Greek Orthodox Church will not normally disclose the following types of information in response to a Subject Access Request:

- **Information about other people** – a Subject Access Request may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data
- **Repeat requests** – where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six-month period of the original request will be considered a repeat request, and the organisation will not normally provide a further copy of the same data
- **Publicly available information** – the organisation is not required to provide copies of documents which are already in the public domain
- **Opinions given in confidence or protected by copyright law** – the organisation does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law
- **Privileged documents** – any privileged information held by organisation need not be disclosed in response to a SAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and his/her lawyer) and is created for the purpose of obtaining or giving legal advice.

The Greek Orthodox Church will provide the information in a clear format that is easily understood and, in a format, suitable for the requesters needs. The organisation may request further details to clarify the exact requirements prior to the start of the one month.

It is a criminal offence under the GDPR for any user to alter, illegally access, deface or remove any record (including e-mails) following receipt of an information request. The Greek Orthodox Church will take necessary action against any individual who is found to have carried out this act, which may result in disciplinary or legal action.

Data Sharing

There are occasions when it is necessary for the Greek Orthodox Church to share data with other organisations or people. Specific details in relation to personal data sharing with third parties can be found in the relevant privacy notice. Please contact Andreas Nicolaou if you have any questions relating to data sharing with third parties.

Disposal of data

The Greek Orthodox Church will retain information about staff, senior members of the church, volunteers and its community for as long as is reasonable and necessary to comply with the law and for legitimate business needs.

For employees, this will include information needed in connection with administering pensions and taxation, for potential or current disputes or litigation regarding employment, in the case of job applicants, in relation to any complaints or claims regarding the selection process, and information required for job references.

The organisation will dispose of data that is no longer needed securely, this means by shredding, pulping or burning for hard copy, deletion etc. for electronic/digitised copy.

The organisation may also use a third party to safely dispose of records on Greek Orthodox Church's behalf. All third parties will be required to provide sufficient guarantees that it complies with data protection law.

Data security breach procedure

The Greek Orthodox Church takes the risk to security loss very seriously. In the event of a data breach or suspected data breach to ensure the organisation responds and manages effectively any breach in line with the GDPR recommendations:

1. on finding or causing a breach, or potential breach, the staff member or data processor must immediately notify Andreas Nicolaou, Treasurer

2. Andreas Nicolaou or a nominated deputy will investigate the report and determine whether a breach has occurred. To decide, they will consider whether personal data has been:

    - accidentally or unlawfully lost, stolen, destroyed or altered
    - disclosed or made available where it should not have been
    - made available to unauthorised people

3. the organisation will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff, senior members or data processors where necessary

4. an assessment on the potential consequences, based on how serious they are, and how likely they are to happen

5. the Greek Orthodox Church will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- loss of control over their data
- discrimination
- identify theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the ICO must be notified

6. Each breach will be documented, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - facts and cause
    - effects
    - action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

7. Where the ICO must be notified, this will be done via the 'report a breach' page of the ICO website within 72 hours

8. An assessment of the risk to individuals will be undertaken. If the risk is high, the Greek Orthodox Church will inform, in writing, all individuals whose personal data has been breached. This will include: set out:

    - a description of the likely consequences of the personal data breach
    - a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

7. The Greek Orthodox Church will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

Training

All staff, senior members or volunteers of the Greek Orthodox Church are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation occur or Greek Orthodox Churchs processes alter.

Monitoring arrangements
This policy will be reviewed every 2 year or early when legislative changes occur.