



St Andrew's Church, Chorleywood

DATA PRIVACY NOTICE

Contents

OVERVIEW	2
SCOPE	2
CATEGORIES OF DATA	2
PROCESSING OF DATA	3
THE EIGHT PRINCIPLES OF DATA HANDLING	3
APPLYING THESE PRINCIPLES.....	4
QUERIES	5
ACCESS	5

OVERVIEW

St Andrew's Chorleywood (St A) uses personal data about living individuals solely to facilitate normal church administration including:

- employee data, electoral roll records, rotas, giftings, visitor information
- lettings and financial records of giving for tax and accounting purposes
- church groups, clubs and other activities
- pastoral care
- the maintaining of data on the Church website
- communication regarding church activities.

St A is committed to the proper and lawful treatment of personal data. All personal data - which may be held by St A on paper, on computer or in other media - will adhere to the appropriate legal safeguards as laid down in the Data Protection Act 1998 and the introduction of the General Data Protection Regulation 2018.

SCOPE

This policy applies to all trustees, staff employed by St A, those contracted and subcontracted by St A and to all volunteers and group leaders – and must be adhered to by them, together with any detailed guidelines published separately for this purpose.

CATEGORIES OF DATA

Data is information which is recorded with the intention that it should be processed on computer or is recorded as part of a relevant filing system (i.e. manual system).

There are two categories of data:

1. **PERSONAL DATA** is information relating to an individual who can be identified:
 - from the data
 - from the data which includes an expression of opinion about the individual*For Example:* electoral roll name and address details
2. **SENSITIVE PERSONAL DATA** is information relating to:
 - racial or ethnic origins of the person
 - political opinions
 - religious beliefs or other beliefs of a similar nature
 - trade union involvement
 - physical or mental health
 - sexual life
 - the commission or alleged commission of any offence
 - any proceedings for any offence committed or alleged to have been committed*For Example:* information held for the purpose of pastoral care

In order to process these two types of data, consent from the individual must be obtained by the organisation handling the data. Explicit consent must be given when it is sensitive personal data. Additional safeguards are therefore in place where sensitive personal data is concerned.

PROCESSING OF DATA

St A will only process data if at least **one of** the following conditions is satisfied:

1. The processing is necessary to further the “legitimate interests” of St A, provided that such processing does not prejudice the “right and freedoms or legitimate interests” of the person concerned. If St A processes data under this condition, there is no requirement to obtain consent from the person concerned, but we will always ensure that St A respects that person’s rights. This includes the rights of those who provide services to St A (e.g. tradespeople).
2. The person concerned has given consent. The consent may be explicit or implicit. By way of an example, a person who emails the church is deemed to give implicit consent for his or her contact details to be stored in such a way that enables the church to respond to the email.
3. In compliance with a legal obligation – for example a court order requiring disclosure of information.

THE EIGHT PRINCIPLES OF DATA HANDLING

St A upholds the eight principles of data handling required by the Data Protection Act. The purpose of these principles is to specify the mandatory conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Trustees, employees and any others who obtain, handle, process, transport and store personal data for or on behalf of St A must always adhere to these principles.

In summary, these principles require that personal data:

1. Shall always be processed fairly and lawfully and shall not be processed at all unless certain conditions are met.
2. May only be gathered for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Shall be adequate, relevant and not excessive for those purposes.
4. Be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose.
6. Shall be processed in accordance with the data subject’s rights.
7. Must be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures.
8. Must not be transferred to a country or territory outside the European Economic Area, 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. St A does not envisage any circumstances in which a transfer of data outside the UK would occur.

Therefore, you can be assured that St A will treat all the personal information that you provide as private and confidential and not disclose any data about you to anyone other than the St A leadership team, employees and group leaders and solely in order to facilitate the administration and ministry of the church, except where required to do so under ecclesiastical regulations as part of the national church. You should note however that there are four exceptional circumstances to the above permitted by and anticipated in the legislation:

1. Where we are legally compelled to do so.
2. Where there is a duty to the public to disclose.
3. Where disclosure is required to protect your interest.
4. Where disclosure is made at your request or with your consent

APPLYING THESE PRINCIPLES

1. All St Andrew's trustees and staff who process Personal Data on behalf of the church will be required to comply with appropriate Data Processing procedures.
2. The Trustees will appoint one of their number as the Data Protection Officer. All questions and concerns in relation to this policy should be addressed to them via Simon Jones in the church office).
3. When personal information is collected for use by St A we will ensure that
 - a. This information is necessary for church purposes
 - b. The information is not kept for longer than it is needed
 - c. Those people supplying the information are aware of this policy and how they can obtain a copy
 - d. All individuals whose names and contact details are published on the St A website will be asked to give explicit consent for their details to be included. We will ensure that data is safely removed from the website and responsibly disposed if the individual concerns requests it.
 - e. Personal information (including photographs) of individuals will not be published on our website without obtaining explicit and informed consent from the individuals concerned or their parents. We will not publish the names of children and young people alongside their photographs.
 - f. We will ensure that all church members and attendees are aware of who to contact to update the information held about them by St A.
 - g. A copy of this policy will be on the church website and is also available from the Church Office Manager.
 - h. All personal information held by trustees, staff and volunteers on behalf of St A will be held and processed in a sufficiently secure manner (whether in paper or electronic form) to prevent unauthorised access (whether by unauthorised church staff or third parties). This means we will:
 - i. Store paper based information in secure, lockable cupboards
 - ii. Use password protections and, if appropriate, encryption of particularly sensitive electronic documents
 - iii. Restrict access to both paper and electronic personal data to those who need to process it for one of the above uses
 - iv. Ensure that personal information is transmitted securely in a way that cannot be intercepted by unintended recipients.
 - v. Access to Church systems will be password protected and only authorised personnel will have access

QUERIES

If you have questions about data protection, please contact Simon Jones (the St A Data Protection Officer) via the Church Office.

ACCESS

St A will provide procedures for access to personal data for all those for whom personal data is held. No charge will normally be levied on anyone (staff, personal members or other contacts) requesting access to their personal data. Any such request should be made in writing and a response shall be provided within one calendar month.

COMPLAINTS, ENFORCEMENT AND DEALING WITH BREACHES

- I. Any complaints regarding Data Protection must be passed immediately to the Data Protection Officer
- II. Any employee, volunteer or trustee who suspects that a breach of the Act has occurred must report it to the Data Protection Officer within 72 hours. Where a breach has occurred procedures for managing breach must be followed.
- III. All employees, trustee and volunteers are expected to cooperate in full with any investigation undertaken by the Data Protection Officer or Information Commissioner into an alleged breach of the Act.

THE INFORMATION COMMISSIONER'S OFFICE

- i. The ICO's role is to uphold information rights in the public interest. The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information.
- ii. The ICO may use criminal prosecution, non-criminal enforcement and audit, depending on the circumstances. The ICO also has the power to serve monetary penalty notice on a data controller.
- iii. Some of the options open to the ICO where there has been a more serious breach of Data Protection Act include:
 - Serve enforcement notices and "stop now" orders where there has been a breach requiring organisations to take (or refrain from taking) specific steps in order to ensure they comply with the law;
 - Issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010, (up to €20m from 25 May 2018).
 - Prosecute those who commit criminal offence under the Act.

Information Commissioner's Office <https://ico.org.uk/global/contact-us> or at the Information Commissioner's Office Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.