

Holy Trinity Gillingham

Guide to the General Data Protection Regulations (GDPR)

These rules come into force on 25th May, 2018 and replace the current UK legislation on data protection (The Data Protection Act 1998). They give individuals much greater rights and protections over who holds their personal data and how it is used. In the church, a PCC is responsible for compliance with these new regulations. Fines for breach of the regulations have been greatly increased.

The GDPR has a number of **underlying principles**. These include that personal data:

- Must be processed lawfully, fairly and transparently.
- Must only be stored with the individual's specific consent.
- Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.
- Should be "adequate, relevant and limited." i.e. only the minimum amount of data should be kept for specific processing.
- Must be "accurate and where necessary kept up to date".
- Should not be stored for longer than is necessary, and that storage is safe and secure.
- Should be processed in a manner that ensures appropriate security and protection.

What this means for Holy Trinity:

Clearly, this has **significant implications** for the way in which we hold data in church, including:

- Personal details of church members
- Personal details of those who have hired our church hall
- Personal details of those we have met through weddings, baptisms, funerals etc.
- Personal details of those who have attended social functions, or which we have obtained through any other circumstance.

Examples of the penalty for **failure to comply** would include:

- For a failure to get parental consent where personal data are collected about a child in the process of providing an "information society service" (e.g. online magazine/newspaper, buying/selling online), a fine of up to 10 million Euros or 2% of the data controller's annual worldwide turnover for the previous year.
- For a failure to provide adequate information to individuals about the data you hold on them or to allow them access to that data, or to comply with their right to have that data deleted, a fine of up to 20 million Euros or 4% of the data controller's annual worldwide turnover for the previous year.

Specific consent is now required for everything that we do. This means, for example:

- We cannot email the whole electoral roll (or everyone we know) with a fundraising request, only those people who have agreed to receiving funding requests.
- We cannot use peoples' email addresses to blanket email about matters they have not *specifically* asked to be kept in touch with. And all email addresses must be in the *BCC column*, so they are not visible to others.
- We cannot contact all baptism families inviting them to "Tea at the Tent" unless they have specifically asked to be kept informed.

Our **Data Security** – the way we store our data - becomes very important.

- We must ensure that the data we keep on individuals is securely stored, whether on paper or electronically, is not accessible to anyone who does not have the right to see it,
- It must be accessible to view at reasonable notice by the person about whom it relates and can be effectively and irreversibly deleted on request.

What we will need to do

- We need to appoint a Data Protection Officer who will take a lead responsibility in ensuring we abide by the new rules.
- We are required to be able to *show* that we are complying with the new rules, so need to develop a data processing policy that details how and why we collect data, and how we store, review and safely delete it when it is no longer necessary
- We are required to have a privacy policy which explains what data we hold, why, how and for how long. This must be available to everyone and be in language that is easy to understand.
- We need new consents to be held on file for members of the church, and for others with whom we are in contact whose data we would like to hold. These must be clear and concise so that individuals know *exactly* what they are signing up to.
- We need to understand exactly *who* we keep data on and *why* we keep it.
- We need to ensure that we understand exactly what data we already hold, and gain consents to continue holding it if we need to, or safely destroy it if we do not. We need to ensure the ongoing safe and private storage of all personal data. This will include:
 1. Going through all the contracts and hall user data, shredding what is not current
 2. Amend the contracts to add a new section on GDPR consents
 3. Going through the filing cabinets, removing rubbish and ensuring they are then locked and the keys are not available except to authorized individuals
 4. Checking with the Lambeth Palace guidelines at <http://www.lambethpalacelibrary.org/content/recordsmanagement> to ensure that we are compliant with the rules on keeping registers, Gift Aid information etc.
 5. Deleting data related to historic weddings, baptisms and funerals, unless permission is received to retain that data.
 6. Asking individuals to reveal what data they hold about other church members etc and decide whether that is appropriate, and whether the necessary consents are held.

7. Create a Data retention map for the church, so we know exactly what is held where, and how it is secured/updated.
- If anyone asks to see the data we hold about them, we are legally bound to respond in no more than one month. It is no longer permissible to charge to respond to this request, unless the request is unfounded, excessive or repetitive
 - If anyone asks to have their data deleted, we are required to comply with this request, as long as the purpose for which the data was held no longer applies. (For example, if someone gave their data by consent so that we might keep in touch with them, they can withdraw consent and ask to have their data removed at any time. If, however, the person is a volunteer or employee for the church, they cannot have data related to that position removed while they are still in post.)
 - If we suspect there has been a breach of the new regulations, we must get in touch with the Information Commissioner's Office within 72 hours (but first we must contact the Diocesan Registrar for advice!)
 - Add a Privacy policy to our website and ensure that all staff and volunteers are aware of it and agree to work within it.

This is a locally produced summary of the Diocesan guidelines and toolkit, which we will be working to. Please take the time to familiarize yourself with the broader scope of the regulations. They can be found at <http://www.rochester.anglican.org/resources/gdpr/>



Holy Trinity Gillingham GENERAL PRIVACY NOTICE

Note: This Privacy Notice is for non-role holders. For PCC members, churchwardens, Deanery Synod Reps, licensed and authorized ministers, clergy, youth workers and other role-holders within the church, see the Role-Holder privacy notice that follows.

Your Personal Data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. From 25th May, 2018, the processing of personal data is governed by the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the “GDPR” and other legislation relating to personal data and rights such as the Human Rights Act 1998.

Who are we?

This Privacy Notice is provided to you by the Parochial Church Council (PCC) of Holy Trinity Church, Twydall which is the data controller for your data.

The Church of England is made up of a number of different organisations and office-holders who work together to deliver the Church’s mission in each community. The PCC works together with:

- the incumbent of the parish (that is, our [vicar or rector]);
- the bishops of the Diocese of Rochester; and
- the Diocesan Office, which is responsible for the financial and administrative arrangements for the Diocese of Rochester.

As the Church is made up of all of these persons and organisations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

Each of the data controllers have their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the PCC on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word “we” to refer to each data controller, as appropriate.

What data do the data controllers listed above process? They will process some or all of the following where necessary to perform their tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to our mission, or where you provide them to us, we may process
- demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you make donations or pay for activities such as use of a church hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process is likely to constitute sensitive personal data because, as a church, the fact that we process your data at all may be suggestive of your religious beliefs. Where you provide this information, we may also process other categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received, political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

How do we process your personal data?

The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

We use your personal data for some or all of the following purposes:

- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To minister to you and provide you with pastoral and spiritual care (such as visiting you when you are gravely ill or bereaved) and to organise and perform ecclesiastical services for you, such as baptisms, confirmations, weddings and funerals;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the parish, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the Church and charity;
- To maintain our own accounts and records;
- To process a donation that you have made (including Gift Aid information);
- To seek your views or comments;
- To notify you of changes to our services, events and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;

What is the legal basis for processing your personal data?

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organisation in the Church of England). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

Religious organisations are also permitted to process information about your religious beliefs to administer membership or contact details.

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties where it is necessary for the performance of our tasks or where you first give us your prior consent. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The appropriate bodies of the Church of England including the other data controllers;
- Other clergy or lay persons nominated or licensed by the bishops of the Diocese of Rochester to support the mission of the Church in our parish. For example, our clergy are supported by our area dean and archdeacon, who may provide confidential mentoring and pastoral support. Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with Bishop's Permissions may participate in our mission in support of our regular clergy;
- Other persons or organisations operating within the Diocese of Rochester.
- On occasion, other churches with which we are carrying out joint events or activities.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access information we hold on you
 - At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
 - There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.
2. The right to correct and update the information we hold on you
 - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.
3. The right to have your information erased
 - If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
 - When we receive your request, we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).
4. The right to object to processing of your data
 - You have the right to request that we stop processing your data. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.
5. The right to data portability
 - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.
 - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).
7. The right to object to the processing of personal data where applicable.

8. The right to lodge a complaint with the Information Commissioner's Office.

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Holy Trinity Church, Twydall Lane, ME8 6JT Email: ann_r@Btinternet.com

You can contact the Information Commissioners Office on 0303 123 1113 or via email

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

Holy Trinity Gillingham PRIVACY NOTICE - ROLE HOLDERS

This Privacy notice relates to those who hold formally appointed roles within the church, e.g. Churchwardens, PCC Secretaries, PCC Treasurers, Deanery Synod reps, Safeguarding officers, employed staff etc.

Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. From 25th May, 2018 the processing of personal data is governed by the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the “GDPR” and other legislation relating to personal data and rights such as the Human Rights Act 1998.

Who are we?

This Privacy Notice is provided to you by the Parochial Church Council (PCC) of Holy Trinity Church, Twydall which is the data controller for your data.

The Church of England is made up of a number of different organisations and office-holders who work together to deliver the Church’s mission in each community. The PCC works together with:

- the incumbent of the parish (that is, our [vicar or rector]);
- the bishops of the Diocese of Rochester; and
- the Diocesan Office, which is responsible for the financial and administrative arrangements for the Diocese of Rochester.

As the Church is made up of all of these persons and organisations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

Each of the data controllers has their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the PCC on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word “we” to refer to each data controller, as appropriate.

How do we process your personal data?

The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

We use your personal data for some or all of the following purposes (depending on the nature of the role you hold – for example, we will not hold financial information about volunteers, just about employed staff): -

- To enable those who undertake pastoral care duties as appropriate (e.g. visiting the bereaved);
- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To deliver the Church’s mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;

- To administer the parish, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the church and charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records;
- To seek your views or comments;
- To notify you of changes to our services, events and role holders
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- To share your contact details with the Diocesan office so they can keep you informed about news in the diocese and events, activities and services that will be occurring in the diocese and in which you may be interested.
- We will process data about role holders for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations, for example to pay role-holders, monitor their performance and to confer benefits in connection with your engagement as a Role Holder. "Role Holders" includes volunteers, employees, contractors, agents, staff, retirees, temporary employees, beneficiaries, workers, treasurers and other role holders.
- We may process sensitive personal data relating to Role Holders including, as appropriate:
 - information about an Role Holder's physical or mental health or condition in order to monitor sick leave and take decisions as to the Role Holder's fitness for work;
 - the Role Holder's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
 - in order to comply with legal requirements and obligations to third parties.

What data do the data controllers listed above process?

- Names, titles, and aliases, photographs.
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving license numbers, vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured, and amounts claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Other employee data (not covered above) relating to Role Holders including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licences/certificates, citizenship, immigration status; employment status, retirement date; billing rates, office location, practice and speciality; publication and awards for articles, books etc.; prior job history, employment references and personal biographies.
- The data we process is likely to constitute sensitive personal data because, as a church, the fact that we process your data at all may be suggestive of your religious beliefs. Where you provide this information, we may also process other categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received,

political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

What is the legal basis for processing your personal data?

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organisation in the Church of England). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

We will also process your data in order to assist you in fulfilling your role in the church including pastoral and administrative support or if processing is necessary for compliance with a legal obligation. Religious organisations are also permitted to process information about your religious beliefs to administer membership or contact details.

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with

- The appropriate bodies of the Church of England including the other data controllers;
- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
- Other clergy or lay persons nominated or licensed by the bishops of the Diocese of Rochester to support the mission of the Church in our parish. For example, our clergy are supported by our area dean and archdeacon, who may provide confidential mentoring and pastoral support. Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with Bishop's Permissions may participate in our mission in support of our regular clergy;
- Other persons or organisations operating within the Diocese of Rochester.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access information we hold on you

- At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
 - There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.
2. The right to correct and update the information we hold on you
 - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.
 3. The right to have your information erased
 - If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
 - When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).
 4. The right to object to processing of your data
 - You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.
 5. The right to data portability
 - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
 6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.
 - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).
 7. The right to object to the processing of personal data where applicable.
 8. The right to lodge a complaint with the Information Commissioners Office.

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Review

We keep this Privacy Notice under regular review and we will place any updates on this web page [add url]. This Notice was last updated in March 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:
The Data Controller, Holy Trinity Church, Twydall Lane, ME8 6JT Email: ann_r@btinternet.com

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.