Fleet Parish Data Protection Policy

Fleet PCC Data Protection Manager: Prof. Robert Smith

Vicar of Fleet and Chair of Fleet PCC: Revd. Mark Hayton

Parish Administrator: Mrs. Rebecca Ratnasamy

Table of Contents

1 INTRODUCTION

1.1 Background

The General Data Protection Regulation 2018 (GDPR), embodied in the UK's Data Protection Act 2018 after Brexit, is designed to protect the rights of identifiable living individuals concerning information about them (known as *personal data*). It covers basic information (such as names and addresses, dates of birth, marital status, etc) and expressions of opinion (such as in job references) but the latter are rare in the parish context. Summaries of various aspects can be found in Annexes A to C.

Failure to comply with the Regulation could expose Fleet PCC to fines, damages and legal costs.

Notification is the process whereby a data controller informs the Information Commissioner (IC) that they are processing (handling) personal data. Each PCC is considered to be a data controller although most should be exempt from notification, whilst the incumbent is a data controller who does need to be registered.

It should be stressed that, even though the PCC is exempt from notification, the remainder of the GDPR still applies to the PCC and everyone in the parish handling personal data.

1.2 This policy

This document encapsulates Fleet Parish's *means of compliance* with the Data Protection Act 2018 (GDPR).

Whilst several helpful documents exist regarding the principles and requirements of data protection at the CofE and Diocese of Guildford level, they do not describe *how* the parish will comply with GDPR. Similarly, the Privacy Notice for the parish describes what data we store, what we will use it for and what we will not do with it, but not how we will ensure this.

This document is intended to explain how we achieve legal compliance in a way that minimises the burden on parishioners, church members, church management and the ministry team.

1.3 Types of data

There are several types of personal data stored by Fleet PCC:

- Contact details of individuals (data subjects) including telephone numbers, postal address and email address, which are stored in the cloud, either in the Fleet PCC account in ChurchSuite (for church members, hall hirers, etc), MailChimp (for mailing of the weekly News Sheet) or in a simple contacts document (for other church contacts such as contractors and suppliers of services).
- More personal information for life events (baptism, confirmation, wedding or funeral) is stored in the Life Events Diary or, if individuals choose to include it, in their Churchsuite account, such as title, marital status, name of partner, etc.
- Planned Giving financial information, which is only accessible to a few people on the Planned Giving Team.
- Photographs of individuals for use in magazines or on the website.

1.4 Consent

Consent (see Annex B) to storage and processing of personal data is essential and it can be either explicit consent (individual actively agrees) or implied consent, where the individual can reasonably be expected to understand that their data will be stored and used for the purposes for which they provided it. The methods adopted for consent is covered more completely in Section 0.

1.5 Rights of individuals

GDPR is designed to protect the rights of individuals, allowing them to be in control of their personal information and how it is disseminated and used. Descriptions of the eight 'rights' of individuals are given in Annex A. In Section 0, this policy describes how the parish addresses those rights using policies on data access, storage and processing.

2 Data access provisions

The parish achieves the majority of its data protection commitments by managing access to data, limiting it to just those who need to know, and by using specialist GDPR-compliant digital applications for cloud storage and data processing – primarily ChurchSuite, MailChimp and Life Events Diary. Table 1 is the key to data access, storage and processing.

Table 1. Summary table of access to personal data based on function within the parish.

<table>
<tr><th>Functional Group:</th><th>Ministry Team & Administrator</th><th>Church Management</th><th>Planned Giving Recorders</th><th>Active Members</th><th>Inactive Members</th></tr>
<tr><td>Comprising:</td><td>Incumbent, Ordained Ministers, Lay Ministers, Trainees, Parish Administrator,</td><td>PCC, Hall Booking Manager, Churchsuite Manager, Website Manager, Parish Safeguarding Officer, Chairs of Sub-committees</td><td>One or two named people who process planned giving, the Treasurer also sees bank statements.</td><td>Rota Overseers, Active Rota Members, Leaders and members of groups and activities.</td><td>Peripheral and occasional attendees, Evensong Choir members, [contractors (eg cleaners)] etc.</td></tr>
<tr><td>ChurchSuite</td><td colspan="3">Have a ChurchSuite ‘User’ account; access to the full ‘Address Book/Contacts’ and ‘Bookings/Customers’ lists is on a ‘need to know’ basis.</td><td>My ChurchSuite account; access only to data made ‘visible’ by the individual.</td><td>No account but can manage communication Cleaners need to see Bookings.</td></tr>
<tr><td>Life Events Diary</td><td>Access to data for processing or communicating</td><td colspan="4">No access to data.</td></tr>
<tr><td>MailChimp</td><td colspan="2">Access to MailChimp Audience list on a ‘need to know’ basis, for weekly News Sheet email distribution</td><td colspan="3">No access to data.</td></tr>
<tr><td>Private Email Address Lists</td><td colspan="2">Communication within Ministry Team or Church Management does not need Bcc but beyond that, Bcc must be used.</td><td>Rarely send bulk emails. For communication with individuals, use ChurchSuite or single email addresses.</td><td>Some legacy rotas are run from private email accounts. Bcc is mandated but this not 100% enforceable.</td><td>Do not send official church emails.</td></tr>
<tr><td>Business Contacts</td><td colspan="2">A single document contains this data, only needed by ministers/managers.</td><td colspan="3">No access to data.</td></tr>
<tr><td>Planned Giving Scheme</td><td colspan="2">No access to data.</td><td>Data stored in secure location (when digital: encrypted and password-protected).</td><td colspan="2">No access to data.</td></tr>
<tr><td>Image store</td><td colspan="2">Images can be viewed for the purposes of obtaining consent and, if given, to put them in a magazine or on the website, with consent being recorded.</td><td colspan="3">Images can only be viewed by these groups once they are in the magazine or on the website</td></tr>
</table>

Data access provisions are detailed more clearly in the following sub-sections…

2.1 ChurchSuite

Ministry Team and Church Management (eg PCC, Parish Administrator, Chairs of sub-committees) can have User accounts in ChurchSuite with 'Read' and/or 'Write' access only to the modules required on a 'need-to-know' basis. Anyone with 'Read' access to the Address Book can see all personal details for all church members on the ChurchSuite database, so this access is not granted except when it is absolutely necessary. Similarly, the Bookings Module contains customers' personal data (unless they are booking for a company) and access should only be granted when absolutely necessary. In general, access just to the Calendar Module is preferred because it does not include access to Customers' data.

My ChurchSuite is the preferred route for access by the active church membership as it gives all the required capability without showing personal data unless it has been made visible in the Church Directory by the individual's privacy settings.

For non-active rota members, such as occasional singers in the Evensong Choir, who are not really part of the church community, their data may be on ChurchSuite and they can view and set their communication preferences using the options at the bottom of the rota-reminder emails but without having access to the full church directory (albeit with privacy settings). They should not be given a My ChurchSuite account.

2.2 Life Events Diary

This is for the exclusive use of the Parish Administrator (and temporary stand-ins) and the Ministry Team and should only be accessible to them.

2.3 MailChimp

This should only include email addresses for the News Sheet mailshot and members of this list can manage the processing of their data with the 'update your preferences' or 'unsubscribe from this list' options in the footer of mailshot emails.

2.4 Personal Email address lists

There are many other reasons why the use of personal emails should be avoided from a data-security perspective.

- The email service provider does not have a formal contractual arrangement with the church and could have access to email addresses.
- Personal emails tend to copy to local hard drives of computers of individuals - these may be shared by other family members who do not have legitimate access to contact lists.
- Some couples or families share email addresses thereby facilitating inappropriate access.
- Some personal email services "autofill" addressees, making it easy to send emails to the wrong person by mistake.

Such issues can be classified as data breaches and may, depending on the nature of the data, need reporting to the ICO

Hence, anyone needing to send official church emails[1] should do this either within ChurchSuite or MailChimp, or using an email address provided by the parish (like our Hall_booking and Office addresses). ChurchSuite and MailChimp hide email addresses automatically but Bcc should be used if emails are sent in any other way.

The use of personal emails for church business is permitted for small scales and ad hoc communications between members where consent for such use has been obtained. For example:

- Church Management and Ministry Team emails to other members of the Church Management *but not beyond*, provided those members of the Church Management have made their emails visible anyway eg on the website). If anyone is uncomfortable with this, they can be given a parish email address (such as the Vicar's!).
- Rota emails where the rota is not on ChurchSuite and rota members have ALL consented to their email address being sent to all other rota members. This consent should be stored and therefore should be in writing or by email. NOTE: If any one rota member does not consent, their email should be sent separately, or Bcc should be used.

2.5 Business Contacts

This address list is kept in a document for use by the Parish Administrator in the Parish Office. It is exclusively information that is publicly available via company websites, etc. Arguably, this means it is not necessary to retain this list but it is retained for convenience and for efficiency of working, handover to other staff or church members, etc. However, as these are business contacts, their contact details are not personal and therefore not covered by the Data Protection Act 2018.

2.6 Planned Giving Scheme

This data is for the exclusive use of an identified 'Planned Giving Team' which includes the Planned Giving Officer and Deputy, plus the Treasurer. Ideally it should be kept electronically and stored on the cloud, preferably encrypted and password-protected. It should only be kept for the prescribed period and then deleted, with only anonymised statistical and financial records kept after that.

2.7 Image Store

Images provided to the parish for potential use, or to provide an official record, should be stored in a central filestore on the cloud rather than on the computers of individual church members.

Church Management can have access to images in the filestore prior to consent being given for wider distribution, for the purposes of obtaining that consent.

Images should only be distributed more widely once consent has been obtained using the prescribed methods, noting that consent is easier for unnamed images of people. Once consent has ben given, those images can be moved or copied to a separate folder for images 'with consent'. Ideally the consent forms should be scanned and stored alongside the image.

[1] An 'official' church email is one that contains a message from the Church Management or Ministry Team sent under the authority of, or on behalf of, a church minister, employee, committee, sub-committee, rota overseer or officer. Hence it does not include an email from an individual acting alone with no authority from the church.

3 Data-processing provisions

3.1 Use of Personal email addresses

In answer to the question: “Can our volunteers use personal email addresses?”, the Information Commissioners Office (ICO) have said that it is not good practice to use personal email addresses to work on sensitive information on the church's behalf. This is because the email [service] provider (eg BT for an btinternet.com account) will have no official relationship with the church (as a Data Processor would) and has no vested interest in the church as a Data Controller.

This does not mean that Church Management and the Ministry Team cannot communicate with individuals (Data Subjects) to their own personal addresses, but that management should use official church email addresses to do so – such as office@parishoffleet.org.uk, treasurer@parishoffleet.org.uk, vicar@parishoffleet.org.uk, etc.

Sending an email from ChurchSuite (eg. to a ‘ministry’ or to rota members or any group of people from the address book), does not use the sender’s email service provider even if the ‘Reply To’ email address is a private one. Therefore, it is deemed acceptable to use ChurchSuite for bulk emails even without using an official church email address. However, it is not appropriate for all receivers of emails to be added to the ChurchSuite Address Book, so this method can only be used if all recipients are in the Address Book.

3.2 Preventing email-address leakage with bulk emails

Ministry Team, Church Management and Planned Giving Officers have full access to the ChurchSuite Address Book so it is assumed that bulk emails can be sent within these groups without needing any further consent.

Rota or Ministry emails from Overseers of rotas should be sent through ChurchSuite’s capability, which hides email addresses where members have not checked the ‘Make Email address visible’ option. Failing that, Bcc should be used to hide email addresses.

An area that is more difficult to control is the inadvertent leakage of email addresses by [church-member] friends of the individual or other members of church teams. The policy is that contact details should not be passed on without the consent of the individual and, to comply with GDPR, that consent should be retained and made available if required. Practically this means that Bcc should be used for any emails sent to, or copied to, more than one email address, otherwise all recipients with see other people’s email addresses.

In the unlikely situation that all recipients of an email have formally consented to their email address being shared with all other members of a group/team, and those formal consents have been retained and are accessible, then it is technically possible to not use Bcc and still remain compliant with GDPR. This is so unlikely to be the case and so difficult to manage the formal consent, especially when new members join the group, that it is not approved of in the parish and Bcc must be used.

Any email communication to more than one email address that does not use Bcc, contravenes this policy and is deemed not to be an official church communication but is just between friends. However, this is not an excuse to avoid following this policy.

3.3 Planned Giving Scheme

Data in the Planned Giving Scheme is very sensitive and must be kept confidential. It is managed by one or two specified people and is also visible to the Treasurer due to the existence of Direct Debits. These people are in the category of Planned Giving Recorders in Table 1.

A process should exist to cover the storage and processing of this data, limiting access to the above-mentioned people.

4 Consent for data storage, transfer and processing

Annex B contains definitions of Consent and Legitimate Interest; these are crucial to this section, which describes how Fleet PCC ensures these rights are upheld.

4.1 Implicit consent

The parish does not need Explicit Consent to store and process data where it has legitimate interest, contractual necessity or a legal obligation (see Annex B) to do so. Thus, explicit consent is not required in the case of any individual who:

- has booked, or is a key person in, a baptism, confirmation, wedding or funeral,
- has joined the church as an active member (on rotas),
- sings in church choirs or plays in church music groups,
- is on the Electoral Roll,
- gives financially on the Planned Giving Scheme[2], or
- has requested to be sent email or hard-copy newsletters, magazines or notifications of events.

These people should assume and expect that their personal contact details will be retained and stored by the parish *for the purposes set out in the Privacy Notice* and according to Table 1. Therefore, explicit formal consent is not required unless the data is to be used (processed) beyond these expectations or unless an individual objects (see Annex A and Section 5.7 Right to Object).

Note that ChurchSuite does give 'Manage Communication' and 'Unsubscribe' options in any rota reminder or email. You do not need to have a My ChurchSuite account in order to manage communication options this way. Also, MailChimp offers 'update your preferences' or 'unsubscribe from this list' options in the footer of mailshot emails.

4.2 Explicit consent

4.2.1 Data storage and processing

For individuals, data types or processing that fall outside the categories mentioned under 'Implicit Consent' above, a formal consent is required and should be stored for future reference. Although it is not recommended, oral consent is legally acceptable but it must be documented immediately and accurately. With ChurchSuite, consent recording is straightforward as a Consent Request can be sent to any individual in the Address Book or to a bulk group of emails, and the responses can be managed. [Life Events also has a facility for this too?]

4.2.2 Data sharing

Consent for transfer/sharing of personal contact data to church members (ie within ChurchSuite) outside of church ministry/management is controlled by the individual in ChurchSuite via their Privacy Settings. If they set any data as 'Visible' this is consent to that data being visible to any Fleet PCC ChurchSuite member.

Before any personal data such as email addresses, are passed to anyone outside the church ministry/management, including beyond the Fleet PCC ChurchSuite members, formal consent will be sought from the individual, giving the reason for the transfer.

[2] Any individual who gives financially on the Planned Giving Scheme should expect the amount of their giving to be stored along with their personal contact details, although they can also expect tighter control of that data – they are told that only Planned Giving Officers and Treasurer will have access to it - the names and amounts appear on bank statements.

4.2.3 Images

Consent is required for photographic images to be made public in hard-copy or online. It makes a difference whether the people in the image are named. For children, the consent should come from the parent until the child has reached 12. Once they are 12, the consent should come from the child and the parent. Once they are 16 or over, the consent just needs to come from the child.

A consent form should be used and preferably signed before the photograph is taken.

5 Addressing the rights of individuals

Annex A describes the eight rights of individuals and the following explains how these rights will be upheld by Fleet PCC.

5.1 Right to be given fair processing information

The Fleet Parish Privacy Notice gives information describing how data will be processed and for what purposes, including to meet legal obligations.

5.2 Right to access

In the event of an individual submitting a Subject Data Request in writing, the parish will be able to provide all the information held by the Fleet PCC in ChurchSuite, Life Events Diary, the database of parish contacts (eg contractors), as well as within the Planned Giving Scheme. Any data held on personal computers or storage owned by persons who may be connected to the church is beyond the official jurisdiction of Fleet PCC and this Data Protection Policy.

Despite the processes put in place to ensure there is no non-consensual leakage of contact details, it cannot be guaranteed that privately held address lists do not contain data for which there is no implicit or explicit consent. It is not practical to list 100% of private church-member address books that may contain contact details of an individual. However, if a rectification (see Section 5.3) or erasure (see Section 5.4) is requested then all Fleet PCC ChurchSuite members will be asked to rectify or erase that data from their private address lists, should that be the will of the individual.

5.3 Right to rectification

In order to mitigate the risk of this process, anyone with a My ChurchSuite account can view and modify their own personal data and privacy settings. It is important that the parish provides and explains this capability, assisting people, where necessary, to view their data. It is also important that data is deleted when it is no longer required to meet any of the parish needs.

A very real risk to do with a frequent event is when an individual changes their contact details and requests that the parish changes all references from the old to the new. Data stored in ChurchSuite and Life Events Diary is easy to change, but tracking the location of old email addresses that may have been sent out in bulk emails, is very time-consuming. The parish requires all bulk emails to use Bcc but this is difficult to enforce and does not completely guard against leakage of email addresses – see comments in Section 5.2.

Finally, a regular audit is undertaken to give people an opportunity to check and amend or delete their data (see Section 6.

5.4 Right to erasure

If an individual requests the removal of their personal data (My ChurchSuite has a ‘Delete Account’ facility which alerts the Data Controller that the individual has requested this), it must be deleted from ChurchSuite, Life Events Diary, the Planned Giving Scheme, the database of parish contacts (eg contractors) and any third party with whom the data was shared must also delete it, unless they were also given it by another route beyond the parish. This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent. For instance, the parish needs a giver’s personal data in order to manage a direct debit and will see the amount given on the bank statements; in order to erase that data, the direct debit would have to be terminated.

5.5 Right to restrict processing

The right to restrict processing means that individuals may request their personal data can be stored but not used. This does not apply when consent is relied upon as the lawful basis for processing the data, which is the case in Fleet Parish.

Note that ChurchSuite does give ‘Manage Communication’ and ‘Unsubscribe’ options in any rota reminder or email. You do not need to have a My ChurchSuite account in order to manage communication options this way. Also, MailChimp offers ‘update your preferences’ or ‘unsubscribe from this list’ options in the footer of mailshot emails.

5.6 Right to data portability

This is not likely to affect parishes.

5.7 Right to object

The right to object provides that individuals have the right to object to data processing in certain circumstances, eg if a parish has relied on legitimate interest to process data without consent (see ‘Implied Consent’ above) and an individual is not happy with this.

5.8 Right not to be subject to automated decision-making

Fleet PCC has no plans to use automated decision-making unless it is based on rules that can be defined and made available; ie. no Artificial Intelligence or Machine Learning methods will be used, only rule-based methods.

6 Audit process

An audit should be conducted annually along the following lines.

Note that ChurchSuite does give ‘Manage Communication’ and ‘Unsubscribe’ options in any rota reminder or email. You do not need to have a My ChurchSuite account in order to manage communication options this way. Also, MailChimp offers ‘update your preferences’ or ‘unsubscribe from this list’ options in the footer of mailshot emails.

6.1 ChurchSuite Address Book / Contacts

This is a process for determining whether data is being kept unnecessarily and should be archived/ deleted, as well as prompting church members to check and amend their personal data.

Go to the Address Book / Contacts list and select ‘Archived’ rather than ‘Active’. Filter (filter button is to the immediate right of the Search box) based on an ‘Archive Date’ more than three years earlier. Select all of these and choose Action ‘Delete’ because they have not been retrieved from the archive in the past three years.

Select ‘Active’ rather than ‘Archived’.

The auditor then needs to find people who should be archived from the list. These are those who have:

- died,
- moved away,
- left or lost touch with our church,
- asked to be removed,

It s also important to check that people still consent to their data being stored and can check and correct the data.

This is best covered by a single communication, by either email or postal mail, informing the person that we have personal data about them and need to know if they would like to:

- check the data ,
- correct the data,
- change the way we communicate with them (eg. by adding an email address),
- change their privacy settings (what is visible to other church members) or
- archive (remove) or delete their data from the church database.

Checking and correction of data can be done in My ChurchSuite or in the parish office.

A suggested email/letter for this purpose is given in Annex D.

A record should be kept of any requests for deletion and the date on which this was done.

6.2 ChurchSuite Bookings / Customers

Go to the Bookings/Customers view and select ‘Archived’ rather than ‘Active’. Filter (filter button is to the immediate right of the Search box) based on an ‘Archive Date’ more than three years earlier. Select all of these and choose Action ‘Delete’ because they have not been retrieved from the archive in the past three years.

Select ‘Active’ rather than ‘Archived’.

Go through each Customer and select ‘View’, then select the ‘Bookings’ tab and change ‘Future’ to ‘All’ to see all their bookings. Then take one of the following actions:

i. if there are no future bookings and the past bookings are one-offs or we suspect they will not book again, select the More… menu item and ‘Archive’. Then say you are sure and proceed. [NB. If the person is in the

main Address Book / Contacts list, you may need to go into 'Edit' and change to 'Not in Address Book' before Archive should be used, just to delete the Customer without deleting the Contact.]

ii. if there is reason to keep them in the Customer list then choose Edit from the menu and enter in the 'Employer' field either the organisation on behalf of whom the booking was made or state another clue as to what the bookings are.

6.3 MailChimp Audience lists

Any MailChimp lists, such as for the weekly News Sheet mailshot, should just have emails and will be updated by recipients if they change their email address. They get ptions to 'update your preferences' or 'unsubscribe from this list' in the footer of mailshot emails. Hence there is nothing more to do.

6.4 Life Events Diary

Some of this information is covered by regulations around Baptisms, Weddings and Funerals. It is only accessible by the Parish Administrator and the Ministry Team but an audit of the process should be carried out to check it is compliant with legislation and regulations in terms of limitation of access and data retention times.

6.5 Personal e-mail address lists

There is little that can be done to check for leakage of email addresses or telephone numbers amongst church members who are likely to be friends anyway.

The main issue here is the sending of 'official' church emails[3] from private email accounts to personal email addresses. There are two possibilities for leakage…

- Failing to use Bcc when copying more than one person where all recipients see all the email addresses but not all addressees have consented to all recipients receiving their personal contact details.
- Use of a personal email account to send to a personal email address where the service provider could potentially see the address and has no formal relationship with the parish.

A reminder should be sent to anyone who is likely to be sending 'official' church emails that they should use Bcc and ideally should use ChurchSuite or a parishoffleet.org.uk email address to send these emails if they are to multiple people. Emails can be easily sent using ChurchSuite from and to everyone in a Ministry, or on a Rota, or those rostered for a particular service. Beyond this, a parishoffleet.org.uk email address should be used and these should be provided for all PCC members and Chairs of sub-committees and, on request, to any other church members.

6.6 Business Contacts

This address list is kept in a document for use by the Parish Administrator in the Parish Office. It is exclusively information that is publicly available via company websites, etc. Arguably, this means it is not necessary to retain this list but it is retained for convenience and for efficiency of working, handover to other staff or church members, etc.

No audit action is required.

6.7 Planned Giving Scheme

Check the process for ensuring this data is only accessible to the Planned Giving Team and check who is in that team. Check that it is kept electronically and stored on the cloud, preferably encrypted and password-protected. Check

[3] An 'official' church email is one that contains a message from the Church Management or Ministry Team sent under the authority of, or on behalf of, a church minister, employee, committee, sub-committee, rota overseer or officer. Hence it does not include an email from an individual acting alone with no authority from the church.

that it is only be kept for the prescribed period and then deleted, with only anonymised statistical and financial records kept after that.

6.8 Image Store

Check that the image store is whole and stored in the cloud, accessible only to the Church Management.

Check that the images in the ‘with consent’ folder do actually have consent forms scanned alongside the images.

Check the process for movement of images with consent onto the website or other publicly accessible locations.

7 Glossary of GDPR terms

Legal terminology can often be confusing, here are some brief explanations of term you'll frequently hear when dealing with GDPR.

7.1 Information Commissioner's Office (ICO)

The ICO is the independent regulatory body which deals with data protection in the UK. They advise on compliance to data protection legislation, handle complaints and may undertake audits of organisations. In more serious cases the ICO can serve enforcement notices, financial penalties and prosecute where a criminal offence has occurred. The most helpful thing the ICO provide is an online Guide to GDPR, which is long and detailed but well-indexed, searchable and a definitive source of information on GDPR.

7.2 Data Subject

The person whom the data is about.

7.3 Personal Data

Any information about a living individual, which is capable of identifying that individual. It can be on paper as well as digital/electronic, and can be images, like photos or CCTV footage.

7.4 Sensitive Information

This is any information relating to an individual's:

- Racial or ethnic origin
- Sexual orientation
- Religious, political or trade union affiliation

7.5 Genetic or biometric data

This is also known as Special Category Information. Note that personal data of our congregations is considered as Special Category because Christian religious affiliation can be inferred because they are members of a Church. This means the data should be handled more carefully and with greater security than 'normal' personal data (although unhelpfully, the law is not specific about how much more securely).

7.6 Data Controller

The legal entity that decides how the data is kept and used. A 'legal entity' can be a company, a charity, a PCC (as a charity), an incumbent or a Bishop. The Church of England, because of the way it is structured and instituted, has a great many 'legal entities'.

7.7 Data Processor

A different legal entity to the data controller, who is actually processing the data, on instructions from the data controller. Note that:

7.8 A data controller can also process data

You can have joint data controllers (two legal entities which share the data)

7.9 Processing

Almost anything you can imagine doing with data counts as ‘processing’: recording, disseminating, adapting, obtaining, destroying, organising, erasing, transmitting, retrieving, combining, altering, holding – all these activities count as ‘processing’ of data.

8 References

9 ANNEX A. Eight Rights of Individuals under the GDPR

People have rights as to how their information is used. These are:

9.1 Right to be given fair processing information

Individuals continue to have a right to be given fair processing information, usually through a privacy notice. Under the GDPR you will also have to explain the lawful basis for the processing of their data; your data retention periods and that individuals may complain to the ICO if they think that there is a problem in the way that you deal with their personal data.

9.2 Right to access

The right to access. Any data subject has a right to access the data which a data controller holds about them, to satisfy themselves it is being processed lawfully. This is known as a Subject Access Request: it may be submitted verbally or in writing; data controllers have one calendar month to provide a copy of the data; and there is no fee for doing this.

9.3 Right to rectification

The right to rectification means that individuals have the right to have their personal data corrected if it is inaccurate or incomplete. If the data has already been given to third parties, you must tell those third parties of the correction. You must also tell the individuals about the third parties to whom the data has been given.

9.4 Right to erasure

The right to erasure gives people the right to request the removal of their personal data. Not only will parishes need to comply with such requests but they will also need to ensure that any third party with whom the data was shared also deletes the data. This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent. For instance, an employer needs an employee's personal data in order to pay the employee, as per their contract of employment.

9.5 Right to restrict processing

The right to restrict processing means that individuals may request their personal data can be stored but not used.

9.6 Right to data portability

The right to data portability gives data subjects the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. It is not likely to affect parishes.

9.7 Right to object

The right to object provides that individuals have the right to object to data processing in certain circumstances, eg if a parish has relied on legitimate interest to process data without consent and an individual is not happy with this.

9.8 Right not to be subject to automated decision-making

The right not to be subject to automated decision-making including profiling.

10 Annex B. Six Lawful Bases under GDPR

The GDPR sets out six lawful bases for processing data— in other words, the legitimate reasons or legal justification for collecting and using someone's personal information. At least one of these (and sometimes more than one) will always apply. Wherever you process personal data, you need to decide what is the most appropriate lawful basis for the processing.

In church contexts it is important to understand legitimate interest. It is very flexible and can apply in a range of circumstances but the disadvantage is that you take on more responsibility for considering other peoples' rights and interests. Consent is a safe option because it places the control with data subjects.

10.1 Consent

Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by clear affirmative action. Even if a parishioner has been on your mailing list for 25 years, the data controller must be able to demonstrate that consent was given. While not common practice, it is lawful to gain consent orally, but you must be very careful to document this immediately and accurately.

It is good practice to offer data subjects options (eg separate tick-boxes for receiving the prayer diary, for service information and for general parish communications) and it must be as easy for them to withdraw consent as it was to give consent in the first place.

The data controller must retain proof of consent being given and withdrawn, for at least as long as the data is used.

You must be able to show that you are complying with the principles by providing evidence.

10.2 Legitimate interest

The processing of data is necessary for your legitimate interests or the legitimate interests of a third party, provided your interests do not outweigh those of the third party. For example, a PCC has a legitimate interest to process personal data of the PCC members, churchwardens, treasurer, etc in order to circulate information about church business so they can carry out their roles effectively. Note with legitimate interest there is a balance/exchange: in this case people offer to hold office, in exchange the personal data is processed to help them to perform that office effectively and the interests are reasonably balanced.

10.3 Contractual necessity

This means that personal data may be processed if the processing is necessary so that a contract can be entered into with the data subject.

10.4 Compliance with legal obligation

This can mean that personal data may be processed if the controller is legally required to perform such processing, such as to comply with the church representation laws, faculty law, tax law, health and safety, safeguarding of vulnerable persons.

10.5 Vital interests

This can be relevant in a life or death situation where it's allowed to use a person's medical or emergency contact information without their consent.

10.6 Public interest

Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

11 Annex C. GDPR's seven principles for personal data

Churches should base all their personal data record keeping on these seven, taken from Article 5 of GDPR. They are set out right at the start of the legislation and inform everything that follows. They do not give hard and fast rules, but rather embody the spirit of the general data protection regime – and as such there are very limited exceptions.

11.1 Lawfulness, fairness and transparency

All individuals should have their personal data processed in a way that is lawful, fair and transparent.

11.2 Purpose limitation

Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

11.3 Data minimisation

Data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

11.4 Accuracy

Data should be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

11.5 Storage limitation

Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (with some stated exemptions for archives for purposes in the public interest).

11.6 Integrity and confidentiality (security)

Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

11.7 Accountability

The Data Controller (see box on p5) shall be responsible for, and be able to demonstrate compliance with, the above six principles.

12 Annex D. Audit communication

The following is a template for an email or letter to be sent out to all members of the church database during an audit.

Dear *******

We hope this finds you well. At the Parish of Fleet we undertake to comply with the Data Protection Act 2018 (and GDPR 2018) using the 'Parish of Fleet Data Protection Policy'. This requires an [annual / 3-yearly] communication with all those on our church database, to remind you that we are storing your personal contact details for the purposes of communicating with you about church services, rotas and activities, and to give you the opportunity to check, change or remove your data from the database. Our full *Privacy Notice* is available to read on our website (parishoffleet.org.uk – under 'Governance' in the menu) or in the Parish Office.

Your data is stored on the Fleet PCC account of ChurchSuite, a GDPR-compliant cloud-storage application and access to the data is controlled according to the *Parish of Fleet Data Protection Policy*. You can maintain your communication and privacy settings and check or amend your data in one of three ways:

a. by having and using a 'My ChurchSuite' account, which we can set up for you if you do not already have one,
b. by asking to access your data and settings in the Parish Office, although this has to be supervised for the purposes of protecting all other data on the ChurchSuite account, or
c. by making an appointment with the parish's ChurchSuite Manager – see the Contacts page of the parishoffleet.org.uk website or mention it at the Parish Office.

If you are receiving this letter in the post, it means we do not have your email address, which makes communicating with you a lot more difficult and time-consuming for us. Ideally, we would like you to give us an email address that we can use to email you. Alternatively, we could provide you with a parish email address and suggest ways in which you could check it and use it for communicating; if that appeals to you, please contact the Data Protection Manager – see the Contacts page of the parishoffleet.org.uk website or at the Parish Office.

If you are happy to continue without making any changes, just make no response to this communication and we will assume that you are consenting to us retaining your data in its current form.

Finally, if there is no reason for us to retain your personal data then we are under a legal obligation to delete it and we would like to be informed if that is the case.

Kind regards

Data Protection Manager – Parish of Fleet