Benefice of Ilminster & Whitelackington Data Protection Policy

Date Written	**April 2018**
PCC Approved Date	**21st May 2018**
Previous Review Date	**October 2020**
Next Review Date	**October 2021**
Review Period	**Annually**
Data Protection Lead Minster **Data Protection Lead W'ton**	**Liz Coleman** **Pam Jackson**

Overview: The church must adhere to the Data Protection Act, and from the 25 May 2018 the General Data Protection Regulation (GDPR), principles as defined by the Information Commissioners Office. A church cannot process data (and therefore cannot use, obtain, dispose of or simply hold personal data) unless it can satisfy one of 8 conditions laid down in the Act.

If individuals can see that their private information is treated carefully and sensitively then this can help build trust for other areas of their lives.

This document has been written using information on the Information Commissioners website: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

What is Personal Data?

'Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' Quote from the Diocese Data Protection Training.

Examples of personal data (not a conclusive list):

- HR records
- Email addresses
- Person's health or other sensitive information
- Employee bank details

A data subject is someone who is living. It does not include deceased individuals or an individual who cannot be identified or distinguished from others.

At the Minster we will ensure:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the data protection acts.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall 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.

What are the exemptions from notification?

Most organisations that process personal data must notify the ICO of certain details about that processing.
However, the Act provides exemptions from notification.
The Office of the Information Commissioner has indicated that churches and charities that only have the following basic personal data would not be expected to register (taken from the Bath & Wells Diocese DPA Policy):

- Church membership list (where individuals have provided their details themselves)
- Gift Aid records
- Accounting records
- Payroll records

A church or charity would be required to register if they hold more than basic data or other forms of personal data, including details of pastoral matters (such as minutes of meetings when individuals are discussed, letters or e-mails sent with any kind of commentary or opinions stated about individuals or pastoral notes).
Churches and charities need therefore to be very careful, if they do not wish to register with the Information Commissioner, to be disciplined in what personal data they obtain and store.

If a church is exempt from notification it must still ensure that information is held in accordance with the principles above.

Practical Application:

Personal information that the church holds about its members (members can choose what we hold):
Full name
Address
Telephone number
Email address

Personal information that the Church requires about employees/ volunteers:
Full name
Address
Telephone number
Date of Birth (Employees only)
Place of Birth (Employees only)
NI Number (Employees only)
Bank details (Employees for wages and volunteers for expense claims)
Medical information (only if it potentially could affect the role they are doing e.g. health condition)
DBS ref number (copies of the DBS certificate must not be retained)
Any other information must not be held as this could be deemed excessive.

Storage of paper and electronic information

- The above information must not be held on a personal computer, laptop or other electronic device unless it can be encrypted and password protected.
- The church office PC has 2 profiles – General and Parish Office. The Parish Office profile is password protected and the password is given to the Parish Administrator, Incumbent and Church Wardens only. Documents are stored on Dropbox and this also has a separate password and the confidential documents have additional passwords.
- On shared devices there must be a password protected separate user profile for the authorised person.
- Devices must be checked for any other device they may be tethered to and untether the device where required, e.g. an Ipad tethered to a laptop.
- All PC's, laptops and other devices holding personal information must install all software updates as soon as possible and ensure that there is adequate virus protection. This is to ensure that we have the current levels of protection and functionality on the device.
- Email addresses – the use of personal email addresses for employees is discouraged and for certain church roles is not permitted. Individuals can have a church email address set up for their role. This is to ensure that there is no risk of personal information being accessed by a third party. It also helps with continuity as the email address can be assigned to the next person in the role and the emails retained securely.
- Dropbox is deemed safe as it is password protected and the documents held on it can also be password protected.
- Employee/ Volunteer information held on paper must be stored securely and safely in a locked cupboard and ensure that no access is available to unauthorised people.
- Once an employee/ volunteer leaves the church or a team then all information held has to be stored for 6 years for record keeping purposes (or 50 years if working with children or vulnerable adults). All information must be marked 'archived' and filed and stored as above.
- If a member of the church leaves then they must be deleted from our records. A record of their name and reason for leaving can be kept for Church of England annual reporting purposes. This must then be deleted after 2 years.
- Church website – we must ensure that the information held on the website does not contain personal information (including photographs – see below) without written consent and that it is hosted within the EU or EEA who also adhere to the data protection legislation.

DBS Database and Safer Recruitment – an electronic list of all volunteers and employees is kept by the Safeguarding Officer on Dropbox (password protected). Access has been given to the Safeguarding Lead and Church Office (for admin support).
The list contains names, contact details, DBS certificate numbers and training courses attended.

Consent is by completion of the DBS form.
Any safeguarding issues are logged electronically, along with scanned copies of any paper documents, by the Safeguarding Officer and allocated an additional password for protection. All paper documents are then destroyed by shredding. Records are kept indefinitely to reduce risk of potential safeguarding issues in the future in line with Safeguarding guidance. Where risk is identified information is shared with the diocese, police and other professional agencies (in line with Safeguarding guidelines).

Safer Recruitment for Employees - Documents are received in the church office and given to an appointed individual. Paper copies are taken for people on the interview panel and then copies (without notes) are destroyed and copies with notes retained as part of the personnel file. Notes taken during the interview, along with any other information obtained through references etc., are retained as part of the personnel file.
All personnel files are stored in a locked cupboard in the church office.
Once an employee leaves the church then all information held has to be stored for 6 years (or 50 years if working with children or vulnerable adults). All information must be marked 'archived' and 'private and confidential' and stored in a lockable cupboard.

Unsuccessful applications, notes and other information are stored in the church office for 6 months (in line with diocese recommendations) and then destroyed securely (shredding).

Safer Recruitment for Volunteers – process is currently being decided by the Safeguarding Team but will follow the same process of handling personal information for Safer Recruitment for Employees.

Identification Evidence for Recruitment – we will never take copies of any documents used to confirm the identity of an individual unless instructed by the Diocesan Safeguarding Officer or HR Consultant. We will write down the documents seen, the relevant code (passport number/ driving licence number) and date of issue of the document. For DBS checks the documents seen are recorded on the secure DBS online application system and no documents are copied.

Electoral Roll – Every year the Electoral Roll is reviewed and church congregation must have the opportunity to check that they are on the list. Information/ consent is obtained by individuals completing an Electoral Roll form and only name and address details are requested. When the list is published we must ensure that <u>names only</u> are featured. People should be encouraged to update any changes of name and address in writing to the Electoral Roll Officer or church office and the electronic list updated accordingly. All forms and letters requesting amendment are stored in a locked cupboard in the church office. Only authorised people to have access to the list whether electronic or paper format. The information provided to the Diocese does not state individual information – just the number of people.

Contact Lists – only one password protected electronic list to be held for the church to ensure its safe keeping and accuracy. All historical paper and electronic contact lists to be securely destroyed by shredding.
Only authorised people to have access to the electronic list.
Details of individuals on this list must not be given out to unauthorised people.
Information/ consent is obtained by individuals completing consent form and only name, address, email address and telephone numbers (where provided) are requested and stored.
If a church member leaves the church then all personal information must be removed from contact lists, etc. and the church/ group leaders contacted to ensure that the individual is removed from their email address lists. A record of their name and reason for leaving can be kept for Church of England annual reporting purposes but then must be deleted after 2 years.
Additional Note - There is currently no publishing of the contact list (as a directory)– if this was required in the future then written consent must be obtained from all individuals involved, choice provided as to what information is to go into the document and the final document must be safely given (in a sealed envelope) to those who have participated only.

Gift Aid Forms - For claiming Gift Aid purposes only. Information held is name, address, telephone number and/ or email address. Information/ consent given by completion of the declaration. Paper copies are held by the Gift Aid Officer and accessed by the treasurer. Paper declarations are kept in a locked cupboard in the Gift Aid Coordinators home. Electronic documents relating to the amounts given by individuals must be password protected and not accessible by unauthorised people. Declarations to be destroyed six complete calendar years after last gift claimed on the declaration.

Baptism Forms – Forms are held on the church office and transferred to an electronic schedule on the office PC which is available to those with access to Parish Office Dropbox Folder. Information held:

- Parents name, address, telephone number and email addresses
- Children's name, address and date of birth
- Names of Godparents.

Paper copies of forms are held in church office in a lockable cupboard. Paper copies of schedules, providing the date and the names of the family only, are held in church office, vicar's office and vestry. Church office PC has its own profile and password and Dropbox is password protected. All paper forms to be destroyed 2 years after the service.

Banns Forms, Wedding Forms and Identification Evidence – Information/ consent given by completion of form and submission of legal documents.
Information required is name, address, telephone number, email address, date of birth and place of birth. Information from the forms is transferred on to the church office PC which is available to those with access to Parish Office Dropbox Folder. Paper copies of forms held in church office and vicar's office in a locked cupboard.
Paper copies of schedule, providing the wedding date and the names of the couple only, are held in church office, vicar's office and vestry. The church office PC has its own profile and password and Dropbox is password protected.
All paper forms to be destroyed 2 years after the service in line with Church of England and UK marriage legislation requirements.
We also must record sight of identification documents for weddings (detailed below).

Identification Evidence for Marriage – we will never take copies of any documents used to confirm the identity of an individual unless instructed by the Diocesan Solicitor. We will write down the documents seen, the relevant code (passport number/ driving licence number) and date of issue of the document. This is then kept with the wedding forms as stated above.

Church and Minster Rooms Booking forms - Consent given by completion of form.
Information required is name, address, telephone number and email address.
Church bookings - Information is held on the church office PC and the Church Diary (event and reference name only).
Paper copies of forms held in church office in a locked cupboard.
Minster Rooms Bookings – Information is held on the Booking Secretary's home PC which must be password protected.
Paper copies of forms held in the Booking Secretary's home in a locked cupboard.
The Church office PC has its own profile and password and Dropbox is password protected.
Paper copies of the Minster Rooms schedule to hold only names and dates of events.
Documents to be destroyed 1 year after the event.

Children - The GDPR brings into effect special protection for children's personal data, particularly in relation to commercial internet services, such as social networking. The church currently does not offer online services to children but if the church did in the future, and rely on their consent to collect their information, we will need a parent's or guardian's consent in order to lawfully use that data. The GDPR sets the age when a child can grant consent at 13 for commercial internet services.
The church should also remember that we have to be able to show that we have been given consent lawfully and therefore, when collecting children's data, we must make sure that our privacy/data protection notice is written in a language that children can understand and copies of consents must be kept.

Consent for children to attend groups, trips out, etc. must still be obtained from the parent or guardian.
As a church we must ensure that all forms holding children's personal information are kept in a secure, lockable place. A lockable cupboard has been allocated in the church office.

Once a child no longer attends a group or once the activity has passed the group leader must pass the information to the church who must retain the evidence in line with Safeguarding and Church of England guidelines (currently 50 years). All information must be marked 'archived' and 'private and confidential' and stored in a lockable cupboard.

Finance – the Church Treasurer holds employee information for the payroll. This includes name, address, email, telephone number, National Insurance number and bank details. This information to be held securely electronically on a password protected PC. Payslips to be issued with a password only known to the Treasurer and employee.
Payments in and out – small business' often use their home address, etc. to work from and we need to take care that invoices and other documents from them are treated with care. Donators information must also be treated with care.
All paper documents must be stored securely and safely in a locked cupboard and ensure that no access is available to unauthorised people. All electronic information must be stored securely on a PC with password protection.
Financial audits – Currently the external auditor does not receive any personal information but if this changes safeguards need to be put in place.

Other Requirements of GDPR: Right to withdraw consent – A church member has the right to withdraw consent to the information we hold about them. This can be total removal of their information (subject to legal restrictions) or just a request to not be emailed about certain information. If a request is received then we must process this immediately and confirm the action has been taken to the individual. A record of their name and reason for leaving can be kept for Church of England annual reporting purposes but then must be deleted after 2 years.

Access to Information Requests – an individual can request access to the information we hold on them.
If a request is received then initially we will confirm what information they wish to see (sometimes this can just purely be a check of an email address). If it is a formal, and full, request to access information then we must complete this within 1 month. There is no longer a fee that can be requested to cover any administration costs for this process.
The information provided includes opinions, voice recordings and manual records (paper notes).
There are very few exceptions and for us this will be under Safeguarding guidelines.

We will follow the ICO checklist and latest guidance at: https://ico.org.uk/for-organisations/subject-access-request-checklist/
To make an Access to Information Request a church employee, volunteer or member must put this in writing to the vicar. The church office will then liase with the vicar(s), church officers and group leaders to collate the information and print information held on the church office PC.

Accuracy of Information – we must ensure that all the information we hold is accurate and easily amended should an individual's information change. An annual review of all employee, volunteer and church member personal information must be conducted in a secure manner. Each individual must be given the information held on them only in writing or email and asked to make any amendments and submit it to the church office for the contact list to be amended. All written or emailed amendments must be kept as evidence in a secure lockable cupboard.

Contact with Individuals – The GDPR has made it clear that organisations must have the consent of an individual to contact them about anything that is not what they originally gave permission for e.g. a baptism family being included in an email about a church event; contacting next of kin about a service other than the funeral of their loved ones.
If the church wants to contact individuals about upcoming events then we must have their written or emailed consent. Verbal is not acceptable. The written/ emailed consent must be kept as evidence for as long as the individual wants to receive information. Most of the church forms have an option for future contact and if an individual wants us to keep in contact they can tick the relevant box. Alternatively they can complete a Welcome Card. If they do not tick the box to stay in touch we must not assume that they have given consent – we must treat this as not giving consent.
An individual has the right to withdraw consent and if we receive a request for this then we will ensure that they are not contacted in this manner again.

Photographs – GDPR has clarified that photos can digitally place someone at a location and therefore form part of an individual's personal data. CCTV is also included but the church currently does not have this. We must ensure that all photos used for social media, church documents, advertising, posters, etc. have the full consent of every individual in it. This must be in writing, using the diocese Photo Consent Form or email and stored in the church office as evidence.

Further Information

Authorised people (as agreed by the PCC):
Incumbent (church office PC and all folders)
Pastoral Team Coordinator (Minster Clergy Folder and Pastoral Team Folder)
Church Wardens (church office PC and Minster Clergy Folder)
Parish Administrator (church office PC and all folders, except Safeguarding issues)

Other Church Leaders with Limited Access:
Safeguarding Officer (for Safeguarding folders only)
Treasurer (financial records)
Group Leaders (limited to contact details about individuals involved with their group only)

Anyone else is deemed unauthorised.

Once any of the above persons leaves their position in the church their access to online and paper records will be terminated immediately.

In line with Diocese recommendations - Data protection will be an agenda item for every PCC meeting and we will ensure that church leaders are kept up to date on any changes to the legislation and have regular reminders.

All personal information must be stored:

- In a lockable building (approved by the PCC), in a safe place where access to the public is not permitted.
- Not in a car – transporting information in a car is acceptable but information must not be kept in a car during the day or over night.
- Protected from fire and flood where possible.

What do I need to do if there is a data breach? In the first instant contact the Church Office.
A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
The GDPR changes makes informing the ICO and the individuals affected compulsory in certain circumstances (e.g. where there is a high risk to the individuals involved, for instance, through identity theft).
There is a Self Assessment tool for the PCC Data Protection Lead or Church Office or to use to clarify the action required.
Under the GDPR, we have to notify the ICO of a data breach within 72 hours of finding out about it. It is important that those in the parish note this deadline and refer to the Church Office or PCC Data Protection Lead about any suspected breaches without delay. If there is any doubt then refer to the ICO website https://ico.org.uk/global/contact-us/ or the ICO telephone support on 0303 123 1113 (local rate).

Our Data Privacy Notice and Data Protection Policy will be held on the church website for all to access.