If using iCloud webmail - To see the BCc field, click the Action icon in the upper right of the window (little gear icon) and select Preferences. Then click Composing and tick the Show Bcc box.

APPENDIX TWO

The Six Data Protection Principles

"data shall be… *[emphasis ours]*

1. … processed lawfully, fairly and **in a transparent manner *i***n relation to the data subject
2. … collected for **specified**, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. … adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed
4. … **accurate** and, where necessary, **kept up to date**
5. … kept in a form which permits identification of data subjects f**or no longer than is necessary** for the purposes for which the personal data are processed
6. … 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"

The Diocese's policy documents below are available to download from www.northamptondiocese.org/data. (Sometimes these will be later versions than what may have been handed out.)

- **General Privacy Notice**
- **Template for Parish Privacy Notice**
- **Stock DP notices and Clauses for parish forms**
- **Diocesan Data Protection Policy**
- **IT, acceptable-use and Passwords Policy**
- **Bring-your-own-device Policy (use of home kit)**
- **Records-retention and Disposal Policy (soon)**

All queries to the Data Protection Manager, Brin Dunsire
Tel: 01844 273337. E-mail brin@nrcdfinance.com

DATA PROTECTION

SUB TVUM PRAESIDIUM

A Guide for Parish Volunteers

July 2018
The Diocese of Northampton

Reg'd Charity 234091

INTRODUCTION 1

This Guide is for you, the unsung army of parish volunteers who keep the Church going at local level, often by working in your own homes, using your own equipment, for the benefit of your parish. Specifically, this is for you if you organise a group, send out rotas, or process lists of names on behalf of your parish. You may find you are being asked, in many cases, to make some changes in the way you work, so that the Diocese and its parishes can move towards compliancy with the new Data Protection laws that came into force at the end of May 2018.

We are anxious not to impose extra burdens on you: but we need to tighten up on how we handle the personal information of other people which is entrusted to us. There is very little new in the Regulations that have come into force, and what is set out here is nothing more than we should all have been doing for years; but all organisations, businesses, public authorities, charities and clubs, are having to take it much more seriously now. You have probably all had a lot of e-mails arriving in your Inbox, asking for your consent to still be contacted by the senders !

Data Protection law is overseen and enforced by the office of the Information Commissioner (ICO). They have made it clear that they are not looking to make life more difficult for churches and small charities; they are more concerned with the bigger companies, marketers and charities who have sometimes been guilty of misusing and selling their huge mailing lists. But we are all vulnerable to someone making a complaint against us, which the ICO has to investigate. We need to be able to show that we have done our best, as far as our abilities and resources allow, to safeguard personal information, which means abiding by the policies and procedures the Diocese has adopted. These are on our website at : www.northamptondiocese.org/data.

And although much of this Guide is about the use of computers and e-mails, do not forget that the Data Protection law also applies to paper records !

Thank you for your patience with this, and for all you do for Our Lord.

Brin Dunsire, Data Protection Manager

Making your PC require a login and password on startup. 10

This is for those who have hitherto not needed to enter a password when starting up their home computer.

Windows 10 *(requires you to have a Microsoft user account password)*
- Hit the Windows flag key and R at the same time
- In the box that appears, type netplwiz (it's "Network Places Wizard") and hit OK
- In the User Accounts box that appears, tick against "Users must enter a user name and password to use this computer"
- Click OK
- You will find that you are required to enter your Microsoft user account password to get into the PC - so if you are not sure you have one, sort that out first !

Windows 7
Click the "Start" button. Click "Control Panel," and then click "Add or remove user accounts" under the section titled "User Accounts and Family Safety." Click "Continue" if the User Accounts Control asks for permission to make the change
Click your account name in the list, and then click "Create a password."
Enter a strong password (see p.3) in the text bars.
Type a password hint into the text bar, and then click "Create password."
Reboot your computer and log in to your account with your new password.

Mac computers
If you wish to make your Mac computer require a login and password on startup and are not sure how to do so, contact Brin.

Blind Copying (see p. 5)

Basically, in all systems , you send the message to yourself (or maybe to the first or main person in your address-list) and put everyone else's address in the "Bcc" field (addressing space) . If you can't see one, see below !

Microsoft Outlook 2016 - If the BCc field is not visible, go to "New Email" as if to write a new message, click on Options in the top ribbon and click on "BCc" in the "Show Fields" section. There is a similar process for Outlook Web App.
Windows Mail (v.17.933*) - you have to click on the letters "Cc & BCc" to the right of "To"
G-mail / Google Mail - When you chooose "Compose", Cc and BCc options are on the far right of the "To" line
ICloud mail (Macs) - If you don't see a "BCc" line, click on "View" then tick next to "Show BCc field".

Creating a new login identity - Windows PCs

This can only be done by the person with "administrator rights" to a computer. If you know you have these, go half way down. If this is not you, here's how to find out who has those rights:-

In Windows 7 -10

Open Control Panel, then User Accounts (it may be called User Accounts and Family Safety). If that doesn't work, type User Accounts in the search box by the Start flag or button.
There should be a list of users, or only one, if you are the only user. It should say next to your name or photo "Administrator", or "Standard user". If you are not the Administrator, you will have to search through the other names until you find who is. And if you can, you may need to contact them and get them to assign you to that role.
If you can't contact them, then unless you are a very confident computer user, you will need to get IT-experienced help for gaining full control of the computer

I am the Administrator of the computer but have forgotten the Admin password.
This is pretty much unrecoverable in Windows 7 / 8 and again you may need some knowledgeable help.
In Windows 10, it is easier because it is based on a Microsoft user account, not specific to the computer itself, and can be re-set via their website; search "How to reset your Microsoft account password"

If, or when, you have Administrator rights:

Windows 10: follow instructions at https://support.microsoft.com/en-us/help/4026923/windows-10-create-a-local-user-or-administrator-account

Windows 7: To open User Accounts, click the Start button, click Control Panel, click User Accounts and Family Safety, and then click User Accounts.
- Click Manage another account. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click Create a new account.
- Type the name you want to give the user account, click an account type, and then click Create Account. We recommend that a user account name should be that of the role, e.g. Secretary, GiftAid not a person's name, . Then it can be "inherited"

Macs - follow the steps at https://www.imore.com/how-create-new-user-account-your-mac

(1) Personal data starts with people's names, addresses, phone numbers and e-mails: it also includes their appearance (photos). Where it goes on to include information about their health, religion, politics or sexuality, it is called "special category" data and has to be even more carefully handled.

(2) This kind of information is *valuable*. It is traded by marketers and criminals. It can be used in fraud and identity-theft.

(3) When we, for good reasons, collect personal information from people, we must:

- Keep it securely and prevent it leaking into the wrong hands
- Only collect the information we actually need, and not keep it for longer than we need
- Ensure it is accurate and up to date.
- Tell people what use we will make of their information (especially if it is more than they might have expected) and explain to them how to find out about their rights as "data subjects"

(4) We do not always need to have their signed consent to "process" their information, especially where we already have it from before 25 May. But if we are going to share it with anyone else outside the parish/ Diocese, or if we are going to send it abroad, or use it in a way that is beyond the initial purpose, then we ought to obtain their consent.

(5) Young people of 13 or over are deemed capable of giving their own consent to the use of their own personal information - or to with-hold it.

(6) If the worst happens and we find that there has been a "data breach" whereby our people's information is (or could be) in the wrong hands, we are obliged to tell them promptly so they can make their own security arrange-ments (such as changing e-mail passwords). This means that we need a back-up copy of the original list !

(7) We have to be careful about answering people who ask us for personal information about another. We need to ask ourselves "Do I know both these people ? Would the subject *want* me to disclose this ? Should I check first ?"

Keeping it secure 3

If it's paper… (lists, sensitive documents)

Don't leave it lying around at home. Put it away when it's not being worked-on. Keep it in a locked cupboard, or if not, somewhere inconspicuous - and not in the same place as your domestic documents, passports etc (which can be targets for burglars if they have enough time). Don't leave such things in cars for long periods, and not on view. And don't take them on holiday !

If it's computer files (lists, spreadsheets, databases, documents)

The kit

We have no right or incentive to tell volunteers what to do with their home computers. But if personal information about parishioners is being held on those computers, it becomes our concern and we have to ask for certain minimal standards of security for those computers and the data on them. These are set out in the "Bring-your-own-device" policy. In summary:

Old computers running on Windows XP or Vista, or old Office programs prior to 2007, are insecure and therefore non-compliant. We cannot insist that you buy a new one, but if you do parish work on an old computer, please speak to your priest who will obtain our advice. Ask also if you use an old Mac computer. Windows 7 users will need to have upgraded by January 2020.

The protection

All computers used for parish work should have a frequently-updated anti-virus program, which will often include a firewall and anti-spyware.

The logins and passwords

Computers used for substantial parish business, even if they are shared with other family members, should have a separate login name and strong password for the parish volunteer. However, If this would be difficult, we will not insist on it if the data held consists only of a short list of rota members. But Gift Aid lists, or a parish census, if held at home, do require restricted access.

The login-and-password are the "front door" and need to be as strong as possible. See Appendix 1 to the **IT Policy** on the Diocese website.

At the time of writing it seems likely that the Finance Office will soon be writing to all Gift Aid organisers to explain the new compliant regime for sending-out and returning the six-monthly Turn-around Lists, so we will not lengthen this Guide with information only relevant to those organisers.

But in general terms, they need to be even more aware than usual of the need for security of these lists when held on their home computers, and when they are printed, and when being sent to the Diocese and the Parish office.

This is also true of photocopies of Gift Aid Declarations (once originals are sent to Finance Office). If possible, these should be stored securely in the Parish office or presbytery, unless needed for current work at home. If they have to be kept at home, they should be filed somewhere very secure so that even a very determined burglar would not find them.

Events, courses and trips

This is usually more the concern of a parish secretary or administrator, but there are some volunteers who organise these things.

There is nothing wrong with a sign-up list which stays on the notice-board only until the event happens, even if it shows phone numbers. The risk of anyone outside the parish photographing, typing-up and selling the list of numbers is minute.

But if attenders have to complete a Booking Form of any kind, particularly if it records health, medical or dietary information, there ought to be a brief DP clause at its foot (adapt the one below) just confirming that the data will only be used for the purposes of the event - and it **must** then be deleted / shredded, say within a month, UNLESS the subject has given their signed consent for you to retain it (e.g. to tell them when next year's pilgrimage is taking place).

Data Protection *- Your personal details given above will be stored and used by the Parish only for the purposes of running and administering the [Jubilee dinner] [Theatre weekend] . They will not otherwise be disclosed outside the parish. Details of how we process your data, and your rights, are on the full Privacy Notice which is on the noticeboard and/or may be seen in the Parish Office and/or on the (Diocesan) website.*

Sacramental classes

Those running them are likely to have lists of names of the children involved, to print attendance-lists, badges, group-lists etc. General principles are that they should contain no more information than is strictly needed, should not be obvious to find for anyone who gains access to your computer, should not be left lying around if printed, and should be deleted / shredded as soon as they are no longer needed.

Forms used for obtaining details of children and their families for baptism or for sacramental classes should be re-designed to include a clear statement of what the personal details will be used for, and notifications that some of them will have to kept permanently in the Parish Registers (canon-law obligation), and some may have to be sent elsewhere and even abroad in future, as when a foreign priest requests a baptismal certificate to support a confirmation class or marriage. (This is more an area for parish secretaries, but catechists may be involved in designing the forms.) Example clauses are in the "Short clauses" document on the website.

If it is the parish's practice to list the names of the children in the newsletter, especially if it goes on the website, the parents should be told that this will happen.

Since they are filling out a form for you, they may as well be asked to sign their consent on it.

Remember that young people of 13 or over have to be asked to counter-sign.

Attendance lists

Recommended by Safeguarding, so we have a record of who has been present on each occasion. Can apply to altar-servers, Children's liturgy, and youth groups as well as sacramental classes. Minimal information, and to be retained permanently in a secure place.

Gift Aid lists and records

These are of particular concern, simply because they are likely to be the second-biggest list of names in the parish (after the census/member database) and are often held and worked-on at home, on volunteers' own equipment.

Quite apart from the general merit of having a backup of all our content on a home computer, in case of theft, failure or infection, we need (as mentioned) to be able to tell our data subjects if their information is compromised. So we need to have an up-to-date copy of the original list !

Unless you are already doing a comprehensive backup of everything, please ensure that the parish data you hold is regularly backed-up, onto an external hard-drive, or a memory stick or rewriteable CD, so long as these are kept elsewhere in the house - locked away, or in an inconspicuous place. And they should NOT be carried around outside the house ! They're too easy to lose !

If you know how to do it, and if the data is not huge, the very best solution is to back-up online ("onto the Cloud") to a password-protected service like Google Drive (see below), Microsoft's OneDrive, or Dropbox.

There are many programs, free and paid-for, that will give you one-touch backup each day and take only a few seconds. Don't rely on remembering to do a full backup once a month.

One good free one is **AOMEI Backupper v.4.1.0**. I use this at home. It is not quite as user-friendly and jargon-free as I would like, but so long as you can get a techie parishioner to help set it up and tell you how to run your chosen backup method, it will do you well.

Another well-reviewed one is **EaseUS Todo Backup.**

Google Backup and Sync is a free add-on for those with a Google account which will back up all your files and folders to Google Drive (and ensure that you always have the latest version on all your devices.) But I don't know how long it takes if used on a daily basis.

There are several inexpensive **paid-for programs** of which I have no experience, so would not wish to recommend one or the other, but any of the ones you might find by searching "Best backup software" will do fine. Windows' inbuilt backup is better than not doing anything, but it will not do an "incremental" backup (only backing-up the files that have actually changed since the last one).

Managing a rota or parish group

This is the biggest issue for some of our parish volunteers. What am I now meant to do about communicating with the members of the rota (readers, Eucharistic ministers, counters, greeters, children's liturgy, whatever it might be) or the group, that I manage (or for which I am secretary) on behalf of the parish ? Can I still e-mail them ? Can I still publish the rota ?

You do not need to obtain fresh consent from people who are already on your rota or group list (so long as it is only ever going to be used within the parish).

You can still e-mail them . But…

E-mails are our biggest headache for data security. E-mails are generally highly insecure. *We need to avoid sending personal or sensitive data using e-mail as far as possible.* However, we have to be sensible. It's not as if you must never name anyone in the body of an e-mail you send. It's the lists of names, or the sensitive documents, we are concerned about.

Multiple mailings

if you, whether as a rota organiser or group secretary, need to send an e-mail to more than two or three people - you should use the "BCc" facility for "blind-copying", so that the recipients cannot see each other's e-mails. And you need to pass this request on to your rota members who may have got used to sending out their own mass e-mails asking "who can cover for me next Sunday ?"

If you have never learned how to use BCc on your particular e-mail method, see page 9.

Stopping sending round open lists of multiple e-mail addresses is not much use if you have been doing so in the past and those messages still exist on many people's computers. *Please ask all your recipients to delete past messages which may have open-view blocks of e-addresses in them.*

The point of this is NOT to stop the members seeing each other's e-mails. They probably already know them, and they need to have them for internal communication. But if a single one of them has their computer hacked-into, the whole block of e-addresses becomes visible to spammers and those who sell them mailing lists.

It is true that using Bcc does not confer complete safety: if the hacker can see all your e-mails, he can probably also see your Contacts List, which is even more valuable. And Bcc'd e-mails are more likely to be caught by a recipient's spam filter, so they may not even get to see them. So we will not count it as a breach if a parish has good reasons for wanting to keep their e-mails "open", But it remains Good Practice.

The Contacts List

Many church rotas need people to be able to contact each other and arrange cover for duties. So they need to have each other's phone numbers and e-mails. But we advise this should should be a separate document from the rotas themselves - in other words, do not print people's contact details next to their names on the rotas.

We should also avoid sending round the Contacts list (when updated) as an e-mail attachment, though this is acceptable if it can be passworded. It may be better to confine these lists to paper prints which are posted out, handed out, or collected from an unmarked box at the back of the Church, to which the members are directed. Some parishes manage without a Contacts List at all.

Displayed rotas

Often found on church noticeboards. In line with the general principle of not disclosing more personal data to the world-at-large than we need to, we suggest confining the names to a surname and initial (or forename and initial) - the people will know who they are.

A suggested clause for your next e-mail to your rota/ group members

***"Data Protection** - Your contact details are held and used only for the purposes of the running of this rota / group. They are shared with the other members of the rota / group to enable internal contact, and possibly with other organisers within the parish who have good reason to need them, but will not be otherwise disclosed outside the parish without your permission. Further information, including a statement of your rights, is on our Privacy Notice on the parish website / available from our office / on the notice-board OR on the Diocese's General Privacy Notice at www.northamptondiocese.org/data. And please delete any e-mails you have had from me in the past which contained an open block of e-mail addresses"*

*Blue indicates text to adapt. T*his only needs to go out once, and to new members as they join. It does not need to repeated in every message.