UPDATA

110010000110
001010011110
1001001100110
0011011110001
110010000110
001010011110

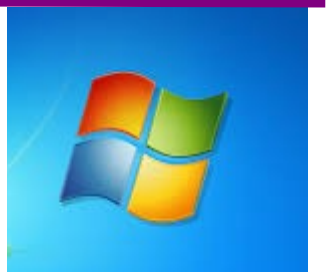
January 2020

This bulletin is intended for Parish Secretaries, priests, deacons, administrators, rota co-ordinators and newsletter editors. Please copy it round. Happy New Year to you all !
I continue to accumulate, from colleagues in other Dioceses and very recently from a course I attended in Salford, a number of Good Practice tips and recommendations, and I hope these will be of help to you as we try to translate the Data Protection principles into the realities of parish life.

Brin Dunsire
Data Protection Manager

DATA PROTECTION

Windows 7 users - it's time to upgrade now



I have been warning of this in all my talks,audits and parish meetings, so it should come as no surprise.

Microsoft recently announced that the Windows 7 Operating System, commonly used and supplied with any Windows computer more than five years old, would no longer be supported by them after **14 January 2020.** This does not mean your W7 PC will stop working after that date, nor will you notice any difference in the short term, but it does mean that computers running under that system will be increasingly vulnerable to viruses and cyber attacks, because Microsoft will not be issuing updates and patches to repair security flaws as they are discovered.
Because of this, it is highly likely that computers running Windows 7 will not be regarded as compliant with the GDPR's requirements about security. The regulations do not say in so many words that we must always have the latest versions of software and operating systems, but they do require us to take into account the "state-of-the-art" in our technical and organisational measures, and this is a strong signal that ageing kit and unsupported software, with security vulnerabilities, will not be regarded as compliant.
The consequence of that is that if any of our parishes suffered a security breach leading to data loss, and it was shown that at the time they were still using Windows 7, we would get very little sympathy from the ICO and possibly a higher penal fine.
You can upgrade to Windows 10 for less that £30 so no parish should have the excuse of unaffordability.
If you find a cheaper offer from a website offering discounts to charities, please speak to the Finance Office before using, as we have had problems in the past with parishes registering themselves as if they were the diocesan Charity.

Photos and live-streaming

I am frequently asked if there is diocesan guidance on the whole issue of taking and publishing photographs at parish events and special Masses. Often, especially when it concerns photographs of children at First Communion masses and the like, it is more of a Safeguarding issue than a Data Protection one. The Catholic Safeguarding Advisory Service CSAS has issued guidance about photography, which you can find by going to the CSAS website **https://www.csas.uk.net/,** then clicking on the top-row tab for the Procedures Manual, then look for Ch. 4 "Creating a safer environment ", then hit "view " which should give you a downloaded Word document, where you will find what you want at section 9

However, from the GDPR point of view, a photograph or image from which someone is recognisable *is their own Personal Data,* and therefore has to be treated by us with as much security and respect for their rights, as any other personal information we hold about them. As with other forms of data, so long as photos are only being kept and seen within the parish, you do not need specific consent to take, retain or print them, but the moment that they are going to be published on the parish noticeboard or website, they become accessible to the general public and the wider world, and you really ought to have the specific consent of those whose images are published - even more so in the case of children.

Most people will not mind the use of their photos taken at parish events, unless you have caught them with a silly expression or at an embarrassing moment, but we have to remember that there are some people among us who would very strongly <u>not</u> wish their images to be put on a website in an identifiable location or context - I am thinking especially of those who have fled from abusive relationships, or who may be being stalked, or political refugees and others who have good reason to wish to keep their location confidential.

So the recommendation is that if you are going to publish photos taken at parish events or masses, you should have a standing announcement in your newsletter saying this is routinely done, and before any photos are taken at each event, there should be a verbal announcement that this is going to happen, so that people can, if they wish, keep themselves out of camera shot or make their objections known to a roving photographer.

In an ideal world you would have a <u>signed consent</u> to the taking and publishing of photographs, (a CSAS/NCSC cosent form is downloadable at **https://www.csas.uk.net/wp-content/uploads/2018/11/PHOTO-1-Consent-to-the-Safe-Use-of-Images-Form-24.10.18.docx**. for appropriate situations) and you *should* try to obtain this if it is the sort of event where those attending have completed some kind of booking form, or as part of routine applications for children to be registered for sacramental classes - but it will often be impractical to get signatures at ordinary parish events, and the best you can do is make the announcement so that people are clear about your intentions and can protect themselves

We would not wish to stop parishioners taking their own photos at parish events. But some of them will want to upload them to their own Facebook or Instagram pages, which can cause just as much of a problem for those who did not want to be pictured. Accordingly, a bulletin announcement prior to an event, or repeated a few times a year, asking parishioners to be aware of such sensitivities, and if possible, to informally ask permission of any person or group who they have photographed, to put the shown image up on the Internet, should prove that we are doing our best to exert some control over this issue. Uploading images of other people's children is <u>Not</u> OK.

All that is said above applies equally to any proposal to "live-stream " a Mass or event. Printed notices advising people where to sit out of shot should be displayed.

Professional photographers engaged by the parish to take photos at events such as First Communion or Confirmation Masses are "Data Processors" in their handling of our people's images. The parish should have a written contract with them, ensuring that they are aware of their GDPR duties to handle our data securely, and not publish the photos on their own websites without our consent. Contact Brin for templates for such contracts, or to review contracts submitted by photography firms

Lodging copies of key passwords

Generally speaking, the point of a strong password that gains access to a parish computer, or to a OneDrive or Google Docs account where sensitive data is stored, is that it should never be disclosed to anyone except its user. However, there is one essential exception to this rule. A note of all passwords used by an individual who does work for the parish should be placed in a sealed envelope labelled on the outside "N.N's passwords", and lodged with the parish priest or the Area Dean. This is because, in the event of the individual's sudden death or incapacitation, the parish and the diocese may need to be able to gain access to that computer, or the individual's Cloud account, so as to remove from them any lists of sensitive data, or retrieve essential uncompleted work
Loss of access to data, because of an unknown password or the simple loss of a filing cabinet key, is as much a notifiable Data Breach, as the data being stolen by a hacker.

Next-of-kin data when arranging funerals

We are often told that when a priest (or deacon, or secretary) obtains details of the next-of-kin and family after a death, there is an expectation that they will retain them, for re-use when a surviving spouse dies some while later. This material may have arrived in typed form in a "Minister's letter" from the undertakers, or it may have been taken down in handwritten notes at an interview, but in either case, Data Protection rules would normally state that the information should be shredded once the funeral has taken place. However, if it is a situation where a surviving spouse is also elderly or in poor health, and to save irritation to the "informing relatives" who have quite enough on their plates, by having to ask for all the information to be repeated on the next occurrence, it will be prudent to say to the informant on the first interview that you will retain all the family information for say 10 years, in case it is needed during that time. If you are having the data collected on a printed form, you can incorporate this notification in the text; otherwise, just tell them verbally , and make yourself a dated note saying "Retention Information delivered and accepted". It is probably not an appropriate moment to seek to obtain a signed consent, and the likelihood of anyone complaining about such details being kept in confidential files for more than a minimum period is pretty remote, so we can afford to be a little informal

Retaining forms as evidence of consent

As mentioned above, one of the key principles of Data Protection is that personal information should not be retained any longer than necessary. Normally, GDPR would say that information captured on booking forms or application forms should not be retained very much after the event or decision to which they relate. This would include the forms by which parents booked their children onto Confirmation classes. However, parishes will often wish to keep the contact details for the family and teenager on file, so as to notify them of youth group events and other opportunities - and so long as the specific consent of the parents, and the young person if 13 or over, has been obtained, that is perfectly in order. But the question has been asked, how do you prove that the consent exists if you have shredded the form they signed ? Those of us who recently attended a DPO training course were assured by an experienced lawyer that parishes are entitled to keep the application forms for a number of years, purely and solely for the purposes of "proving consent". If you can be bothered, the ideal solution would be to cut-off the foot of the form showing the signature, and just keep all these slips of paper with one specimen of the form, or even to compile a dedicated list stating that the named parents signed a form exactly like the specimen on such-and-such a date ; but that is probably procedural overkill, and if you have no problem about keeping a batch of confirmation forms in a file, stored securely of course, then you have justification for doing so.

Bulk e-mails and the “PECR”

The "Privacy and Electronic Communications Regulations 2003" is a bit of a mouthful, and these UK regulations, implementing an EU Directive 17 years ago, were mainly aimed at telecommunications operators and Internet Service Providers, but they have at least one area of Impact on parish life. They prohibit the sending out by e-mail of “unsolicited marketing messages". It is not *obvious* that this would affect a parish in its ordinary activities, though it might well wish to send out an email to all its parishioners whose details were collected on a parish census, to notify them of parish events, save money on posting out a monthly parish magazine, tell the confirmation candidates about a youth event, etc, Surely none of this can be called "marketing"? After all, we are not attempting to sell anything - merely to advise known interested parties of our services, which as often as not are free of charge

Unfortunately the understanding of "marketing" in these regulations is extremely wide, and basically Includes anything which promotes the communicating organisation or shows it in a good light. So anything beyond the most basic administrative messages (e.g. "we acknowledge with thanks receipt of your kind donation, and invite you to sign the accompanying gift aid declaration to cover it") is prohibited unless you have specific consent to send "marketing material" to individuals. Because it is difficult to predict with certainty whether a particular type of message would be understood as "marketing" by the ICO or the courts if anyone were to complain, it will *always* be prudent to obtain signed consent to email communications at the same time as you collect the original data - probably in a parish census form or on an application form of some sort. And your people have to be told that they have the right to withdraw consent to e-mail communications at any time, and then you have to be able to amend or filter your e-mailing list so as to exclude anyone who wishes to withdraw from it.

None of this stops you sending out the same information by post, if that is a practicable alternative, as you can tell by the amount of junk mail that we all receive ! Please remember, though, that if you *are* contemplating a mass mailshot, and engage a printing or "fulfilment" firm to do this for you, they will require you to send them your addressing database and will therefore constitute "Data Processors" just like the photographer above-mentioned - written contract needed – as it would be for any printer whom you wanted to use to print labels for e.g. the Offertory Envelope boxes.

Nor need you worry about this preventing a rota organiser, or choir director, sending out routine informative e-mail messages to a small number of people. This is not the kind of activity it was intended to curtail.

Wi-fi routers

It is a common situation, that if a parish hires out its hall for a private party, a dance group or local charity, they are likely to ask you for the password of the parish Wi-Fi, so that their staff and guests can use their smartphones and laptops. The trouble with this is that allowing outside users into the parish Wi-Fi network could, in theory, enable a knowledgeable and determined person to gain access to the parish computer and all its confidential files. So one answer is to create a "guest" Wi-Fi account with a different password, so that they can get the Internet access they need but cannot go any further into the parish network . Another is to set up a Demilitarised Zone (DMZ) on your router, which again allows Internet access but prevents outside users penetrating the parish network. If you do not have an IT whiz in your congregation who knows how to do this (it is apparently fairly straightforward on most modern routers) Deacon Jim Hannigan is willing to offer advice.
deaconjimhannigan@northamptondiocese.org