Safer Use of Technology

New Technologies, New Opportunities

New technologies offer tremendous opportunities to reach, communicate, evangelize and engage with those involved in the Catholic Church and those in our communities who may have an interest in the church. The internet, mobile phones, social networking and other interactive services have transformed the way in which we live.

New Technologies, New Risks

Along with the many benefits of modern communication technologies, there are risks. The anonymity and sense of distance inherent in online communication can make it easier for people to say things they would perhaps not say in the presence of somebody, and to feel less remorseful about online harm caused.

The online world makes it easier to engage in criminal offences and abuse. It enables easy creation of, access to, use and dissemination of pornographic and abusive images and videos, easy access to children and adults who are vulnerable for the purposes of grooming, ease of presenting as someone else and greater potential for online bullying and abuse.

The Use of Church Computer Equipment to Store Information

Diocesan or congregational policy and procedure on the use of its own computer equipment and the storage of information on personal computer equipment must be followed. Electronic records, like paper records, should be kept in accordance with the record retention schedule.

Creating and Managing Church-Related Websites and Social Media Pages

Websites or social media profile pages are useful means to engage large groups of young people. The following are recommended guidelines to promote safety online. The development of websites should be in accordance with diocesan or congregational policy and procedure. In the absence of local guidance, the following good practice guidance can be followed:

- Parish websites and social media profiles should be approved by the parish priest and should be disclosed to the diocese.
- Where there is user-generated content, the site should be moderated/ administered by a minimum of two adults.
- Personal sites should not be used for diocesan or parish programs; separate sites should be created for these.
- Passwords and names of sites should be registered in an encrypted document in a central location in the parish and/or diocese as appropriate. More than one adult should have access to this information.

Accessibility of Websites and Social Media Pages

Websites need to be accessible to all and adjustments could include functions that change contrast, text size, or offer an audible alternative when viewing web pages.

Examples of such adjustments can be found at the **DisabledGo website**;

Access to the internet

Diocesan or congregational policy and procedure must always be followed. Where children, young people and adults have access to the internet using church computers, other electronic devices and WIFI as part of Church activities, the event leader has a duty to ensure that:

- Use of the equipment and WIFI is supervised and/or monitored.
- Measures are in place to ensure that the likelihood of accessing inappropriate materials is reduced e.g. firewalls, parental controls and software to filter out internet material.

Social Media and Social Networking

The internet has evolved to become an increasingly dynamic and interactive medium led by social networking services. The convergence of technical and communication platforms means that users can now interact with each other across multiple platforms and devices, such as mobile phones, games consoles, watches and PCs (laptops, notebooks, tablets etc.).

Social media includes any site or forum that enables sharing of any user-generated content. These services are very popular with children and young people and bring together pre-existing interactive technologies and tools (e.g. email, messaging, chat, blogs, photographs, music, videos, gaming, discussion forums) in a single service through for example Facebook, Twitter, Instagram, WhatsApp, Snapchat and live messaging services such as Facetime, Duo and Skype, and so on. It is the way in which these different technologies are used that makes them 'social'.

Good Practice in Relation to Social Networking:

- Government guidelines recommend children under 13 years should not be using social media.
- All users should be made aware that their personal details e.g. last name, address, school, passwords, e-mail address and telephone numbers are private and should not be disclosed unless approval is given by the event leader.
- All users should be made aware that they should never send images of themselves or others and should be wary of people misrepresenting themselves in chat rooms.
- All users should be aware that they should advise a leader about anything on line that makes them feel uncomfortable or concerns them.
- Children and young people should be advised to always tell an adult they trust about communications that make them feel uncomfortable or where they have been asked to keep communication secret.
- Children and young people should be made aware that they should advise a leader and their parent or carer of a request to meet up with someone they have met on line, not to make plans to do so without alerting an adult and never to go alone to such planned meetings.
- Children and young people should be advised of a code of conduct for using chat rooms.

'CHAT' is a simple code that can be used for remembering some rules around the use of the internet and social media.

C	**CAREFUL** – People online might not always be who they say they are.
H	**HANG** – Hang on to your personal information. Never give out your home address or other information.
A	**ARRANGING** – Arranging to meet can be dangerous. Never arrange to meet someone unless you are sure who they are.
T	**TELL** – Tell your friends or an adult if you find something that makes you feel uncomfortable.

The Use of Social Networking for Communication with Children and Young People

The diocesan, congregational or organizational policy and procedure on the use of social networking for communication with children and young people must be followed.

- In the absence of a local policy and procedure the following good practice guidance can be followed.
- If a group, parish or other body decides that the most effective way of communicating with children or young people is via a social networking site, it is advisable to set up a custom account in the name of that group, parish or body.
- How the media is used should be made explicit to children and young people, and permission for communicating directly with children and young people via social media must be sought from parents.
- Social media sanctioned by church organisations or personnel should be moderated by at least one adult familiar with safeguarding procedures, and a minimum of two adults in total.
- Parents should approve and have access to all sanctioned social networking that is directed at children and young people.
- Children or young people should not be communicated with via social media for any other reason than the specific ministry for which parental consent was obtained.
- All communication, including online, between an adult and a child or young person should take place via the most public means of communication appropriate without jeopardising the prevailing data protection legislation.
- For matters that are sensitive or private, online communication should be avoided due to the possibility of misunderstanding and, if used, parents should be included.

Personal Social Networking Accounts

The diocesan, congregational or organizational policy and procedure on the use of personal social networking accounts must be followed.

In the absence of a local policy and procedure the following good practice guidance can be followed.

Many clergy, religious, lay persons, employed staff and volunteers have a personal online social networking presence via social media platforms, personal blogs and websites. As a member of the Church, personal social networking (e.g. Twitter or Facebook) should always reflect Catholic values and should contain content that is universally appropriate to any possible user. Whether public or private, all individuals should understand that they are witnessing to the faith through all their social networking and as such, personal views should be cited as such to avoid misunderstandings.

Although there may be reasonable overlap between the personal and spiritual realms in communications between adults (with full capacity) within the Church, this is never the case with children, young people or adults at risk.

- It is never appropriate to use personal social media accounts, phone numbers or email addresses to contact children and young people without parental consent, or with adults who lack capacity to give their consent.
- It is not appropriate to send or accept 'friend requests' from children, young people or adults who lack capacity to consent from personal social media accounts.
- The strictest of privacy settings should be activated on all personal social media accounts and individuals must take personal responsibility to ensure that their content is appropriate to those that can see it e.g. language, jokes, opinions.

Church Website and Social Media Monitoring and Reporting

The diocesan, congregational or organizational policy and procedure in respect social media monitoring and reporting must be followed. The following is good practice guidance:

- Suitably skilled adults should be appointed to monitor the content of websites and act to remove offending material.
- Any discovery of inappropriate use (of a safeguarding nature) of social networking sites, computers, email or texting should be reported to the parish Safeguarding Representative or Safeguarding Coordinator who will report to the relevant person within the diocese, parish or religious congregation.

- Unofficial sites that carry the diocesan, parish or religious congregation's crest or logo should be reported to the Diocesan Communications Office, Parish Priest or relevant person within the religious congregation. Any misinformation found on a site, such as Wikipedia, should also be reported to the Communications Officer or relevant role.
- Any forum that includes user-generated content should be moderated on a regular basis to prevent libellous, rude or inappropriate remarks so that the information can be removed.
- Consider adding the CEOP help button to your site. The CEOP help button gives access to help on viruses, hacking, online bullying and enables reporting of people acting inappropriately online www.ceop.police.uk.

Administrators and Moderators

The diocesan, congregational or organizational policy and procedure in respect of administration and moderation must be followed.

- In the absence of a local policy and procedure the following good practice guidance can be followed.
- Adults moderating sites and adding user-generated content should take care:
- To appreciate that even personal communication by church personnel reflects the Church.
- To write in the first person.
- Not to claim to represent the official position of the organisation or the teachings of the Church, unless authorised to do so.
- To identify themselves with real, full names.
- Not to divulge confidential information about others.
- To avoid posting personal, political or negative content online.
- To ensure that text and photographs posted are in the public domain and not subject to copyright infringement.
- To not cite others, post photographs or videos of them or link to their material without their explicit permission.
- To practice Catholic teaching and morals always.
- To always report any form of bullying, trolling or libel to the diocese, parish or religious congregation.
- To always report any concerns about any inappropriate behaviour online.
- To always report any suspected online grooming.

The Use of Email and Texting (SMS)

The diocesan, congregational or organizational policy and procedure on the use of email and texting must be followed.

In the absence of a local policy and procedure the following good practice guidance can be followed.

The benefits of email and text messaging (Short Message Service - SMS).

Emailing and SMS are a widely accepted and attractive means for communication that people of all ages rely upon. Benefits of communication by email and SMS include quick and easy communication without delays and reduced postage costs.

Email and SMS can be helpfully used in relation to Church activities to:

- Send quick messages to individuals such as reminders about or changes of arrangements for activities.
- Broadcast the same message to a wide-ranging audience such as promotion of an event.

Agreeing the Use of SMS

The need or benefit of using email and SMS and approval of its use should be agreed with the leader of the Church group or activity. The approval should be documented along with the following:

- Identification of the need or justification for the use of email and SMS.
- Identification of when email and SMS will be used.
- The agreement to the use of the service by its intended recipients.
- Clear identification of the associated risks and of how these risks are managed.
- Storage of messages sent and received.

Consent

Written consent must be gained from adults at risk or the parents of a child or young person (up to 18 years of age) and for 16 and 17-year olds, the young person's consent should also be sought, prior to the commencement of email and SMS messaging taking place.

When written consent is being sought the potential benefits and risks should be explained before deciding on whether or not to receive email and SMS communication.

Consent to be contacted by email and SMS can be withdrawn at any time and must be implemented without delay.

Risks

The following risks must always be considered:

- Emails or SMS not reaching the intended recipient.
- Content sent in haste that cannot be retracted.
- Storage of content as 'records'.
- Information not being sent securely via the internet.

Safer Practice

Using Emails and SMS to communicate with children, young people and adults at risk should be done using an organisational account and organisational equipment. It is not recommended that personal telephones or accounts be used for communicating with children and young people or adults at risk.

A generic email address or telephone number associated with the role in question (voluntary or not) maintains appropriate boundaries.

Where more than one leader or helper needs to communicate with group members, it might be appropriate to set up a generic shared email account and have a shared mobile telephone. The benefits of this are that:

- Communications can be easily reviewed by other leaders or helpers in the event of enquiries.
- The need for action on any matter can be easily shared and delegated.
- Communications can be picked up in the event of sickness or other absence.

- All correspondence and data is stored securely in one place.

Email and SMS should not be used to transmit person identifiable information, confidential or other sensitive information.

Those to be included on group email addresses must give their consent to be included in group communications.

The BCC field should be used for group emails to avoid recipients receiving the contact details of other recipients.

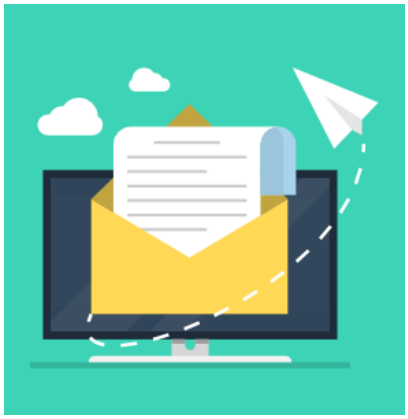
When sending messages, emails or texts to young people, parents another group leader or helper should be copied into all communication. All communications should be strictly regarding a specific Church activity and not be personal conversations, contain pictures, jokes or anything of a personal nature.

Emails or texts from young people, other than those directly related to your role within the Church or the activity you are concerned with should not be responded to.

The Safeguarding Representative or Safeguarding Coordinator should be advised if somebody receives any inappropriate texts, images or emails.

Copies of all texts, WhatsApp chats, personal messages and emails should be kept on file.

Newsletter Mailing Clients



A potential way of managing bulk communications and protecting personal data is to use a newsletter mailing client. The issuing of newsletters should be in accordance with diocesan or congregational policy and procedure.

Useful links and Resources for Internet Safety

The UK Council for Child Internet Safety (UKCCIS) is a voluntary organisation chaired by Ministers from the Department for Education and the Home Office. UKCCIS brings together over 180 organisations and individuals from government, industry, law enforcement, academia, charities and parenting groups. Some of the organisations UKCCIS works with include: Cisco, Apple, Sony, Research in Motion, the four largest internet service providers, Facebook and Microsoft.

The Child Exploitation and Online Protection Centre (CEOP) has numerous resources for parents and carers and children using the internet; there are several video tutorials on the THINKUKNOW site which is part of CEOP.

Lucy Faithful Foundation is a registered child protection charity which works to prevent child sexual abuse. It runs 'Stop It Now!' and 'Parents Protect.

Stop It Now! reaches out to adults concerned about their own behaviour towards children, or that of someone they know, as well as professionals, survivors and protective adults. Stop It Now! runs a Freephone confidential helpline.

'Parents Protect' is a site to help parents, carers and other protective adults with information and advice to help them prevent child sexual abuse.

Catholic Youth Work has detailed guidelines on the use of social networking sites.

Internet Matters gives advice on parental controls and is a great way of preventing children accessing unsuitable content online.

Childnet International is a multi-lingual resource site which has a guide on protecting your privacy on 'Facebook'.

The NSPCC has useful resources for keeping children safe online including sections on Cyberbullying and Sexting. Reporting and Monitoring.

Photography and Filming

The diocesan, congregational or organisational policy and procedure on the use of photography and filming must be followed, taking into account data protection requirements.

In the absence of a local policy and procedure the following good practice guidance can be followed.

The General Data Protection Regulation 2016 ("GDPR")

Whenever a person's image is captured, be it by camera, video, web camera, mobile phone, or CCTV, and that person can be identified, the image is likely to be considered personal data. This means that the image must be processed in line with the data protection principles. Processing means anything that is done to the image for example recording it, using it or sharing it.

For the Church to use images of people that enable those people to be identified, they need a lawful basis (see Article 6 of the GDPR):

- The person (or parent) has provided their consent to the processing of his or her personal data for one or more specific purpose.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (e.g. preventing or detecting a crime or catching an offender (this is relevant when using CCTV cameras)).
- The photographs are necessary for the purposes of the legitimate interests pursued by the controller (e.g. educational purposes) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the person which require protection of personal data, in particular where the data subject is a child or vulnerable adult.

Data Subjects' Rights

Individuals have several rights under the GDPR in relation to how their information is processed. These rights include the right to:

- Request a copy of the personal data (including images) held about them; this is known as a Subject Access Request (Article 15 of the GDPR);
- Prevent their personal data being used in a way which causes them unwarranted damage or distress (Article 21 of the GDPR);
- Prevent their personal data being used for direct marketing purposes (Article 21 of the GDPR);
- Compensation if they have suffered material or non-material damage as a result of their personal data not being processed in accordance with the DPA (Article 82 of the GDPR);
- Have inaccurate or misleading information held about them corrected or destroyed (Article 16 and 17 of the GDPR).

Dioceses and Religious Congregations should identify a member of staff who will be able to deal with these situations as they arise.

More information can be obtained from the Information Commissioner's Office.

Privacy Notices

The GDPR states that personal data must be processed fairly, lawfully and in a transparent manner. To comply with this, if the Church wants to take an image (e.g. photograph) of someone or to record their activity, they need to tell the person:

- That photography and/or filming will take place.
- Why they will be taken.
- What will be done with them.
- Who may see them.
- Any non-obvious consequences; for example, if the photograph and/or film is going to be used on a website, in a newsletter, or on a televised programme.

This is known as a privacy notice. Privacy notices must be concise, transparent, intelligible and easily accessible in terms of language used. Privacy notices must be issued at the time the images are collected and always before they are used.

If photography or filming is going to take place, people should be told beforehand and given the opportunity to object or simply move out of the picture. This is particularly important if the images are to be used by a journalist or a media company.

It will not be considered fair or lawful if images are collected for one reason and then later are used for something completely unconnected, without going back and gaining consent for the additional use or being able to rely on another processing ground in the GDPR for that additional use.

Issuing a privacy notice is not the same as asking for consent.

Consent to the Use of Images

Consent must be gained from the data subject. Individuals must be informed that photography or filming is taking place and the specific contexts in which the image will be used, as described above

If an existing image is to be used for a different purpose than the original intention, the individuals should be notified of its re-use and the purpose for which it is going to be used again.

If an image is to be used on a website or for commercial purposes, this should be explained to the individuals and consent from those in the image must be obtained if they can clearly be identified.

Informed Consent

The person giving consent must understand why their image is being used, who may see it and any implications that may result from using or disclosing the image. Consent must be clearly given. Consent is good practice and can be expressed either verbally or in writing but consent in writing is recommended. Written consent is preferable because it reduces the scope for subsequent dispute.

Individuals have the right to withdraw or limit consent at any time.

Consent for Images of Children and Young People

Consent for children and young people under the age of 16 must be sought from parents (this includes those with legal responsibility for the child). Young people over 16 years of age are usually considered to be competent to give consent and so consent must be sought from them directly, and if felt to be necessary, also from parents/carers.

A template consent form is located in the Forms Library.

If an image is published without the consent of the individual or parent when consent should have been obtained, a complaint can be made to the Information Commissioner's Office. In some cases, this could result in a fine, enforcement action and damages being awarded to the complainant.

Consent for Images of Groups

General images taken of groups, where individuals cannot clearly be identified, do not require organisations to obtain consent from every person featured in the image. However, the fact that such images may or will be taken at any particular event should be made clear to people attending the event.

Photography and Filming at Activities

The Data Protection Act 2018 (DPA) and the GDPR do not prevent parents or other family members from photographing their children at activities. Settings are entitled to decide whether or not they allow photography to take place on their premises, however, it should not be banned for fear of breaching the DPA. The DPA and GDPR do not apply to parents or other family members taking pictures of their children for their own personal use, for example to go in a family photograph album. When taking photographs, parents do not need to obtain the permission of the other parents in case their child appears in the picture.

Inappropriate Photography and Filming

When taking photographs or filming children and young people, the photographer must make sure that the children and young people are appropriately dressed. Photography of children in PE or swimming costumes should be avoided except in appropriate circumstances, for example a swimming performance review. Attention should also be paid to using appropriate camera angles and the use of zoom and cropping for all types of photography or filming.

If someone is suspected of taking inappropriate or unauthorised images, they should be asked to stop and leave the site. The incident should be recorded and, if appropriate, reported to the Police.

Storing Images Safely

Personal equipment (phones, cameras, laptops) should not be used to take or store images. Church equipment must be used for this purpose.

Church equipment should be stored securely in a locked cabinet and a log should be kept of who has used the equipment, on which date and, for which purposes.

Images, especially of children and young people, should not be stored on un-encrypted portable equipment such as laptops, memory sticks and mobile phones.

Storing personal information on these devices is not considered secure. The Information Commissioner does not look favourably on organisations which permit personal data to be downloaded onto unencrypted equipment.

Photographs and films should be downloaded onto a secure electronic location and deleted from the device at the soonest opportunity available.

Electronic images should be held in a protected folder with restricted access, to make sure that only authorised individuals can access them.

Non-electronic photographs and videos must be stored securely in locked drawer or cabinet and destroyed in accordance with the record retention schedule.

Timescales for Use

There is no official guidance on retention periods for images, so it is up to each individual church to decide how long they need to keep images and how they are going to securely destroy them when they are no longer needed. If a church decides the images are required for historical purposes, for example in the archives, these can be retained for as long as is considered reasonable and necessary.

Subjects should be informed about the length of time that a given image or film will be kept and used. A typical period is between 3-5 years.

If the Church wishes to prolong the period of use of the image or film, they will need to request the permission of the subject or parent as appropriate to do so.

If the church wishes to use the image or film, for a different purpose and in a different manner than originally stated, they will need to request the permission of the subject or parent as appropriate to do so if the further use was not compatible with the original processing notified to the individuals.

For this reason, secure logs should be kept in relation to each image on file complete with:

- Contact details.
- Expiry dates for use.
- How and where they are being used.
- Where to locate them if they are being used online (i.e., the relevant urls).

Files should be checked regularly for the purpose of destroying images that have expired, and ensuring that they are removed from circulation.

Sexting

It is illegal to take, store or disseminate a sexually explicit images and videos of a child under the age of 18 (Sexual Offences Act, 2003).

A young person or an adult is breaking the law if they:

- Take an explicit image or video of themselves or a friend.
- Share an explicit image or video of a child (anyone under 18), even if it is shared between children of the same age.
- Possess, download or store an explicit image or video of a child (anyone under 18), even if the child gave their permission for it to be created.

It is also an offence where a person above the age of 18 intentionally communicates a sexual communication with an individual they do not reasonably believe to be over 16, for the purposes of sexual gratification, or, alternatively, where the communication is intended to elicit a sexual communication from the recipient.

There are many reasons why a young person might share a nude or semi-nude picture of themselves. They may want to 'belong' to a social group, interact with others and explore sexual feelings and get attention on social media. They may also find it difficult to refuse if someone asks them to send them one.

Once images are passed on electronically, control is lost over what happens to them, where they are posted and who sees them. Other people may use sexually explicit images of a minor to bully them, to blackmail them and to cause harm to them.

Response to Sexting

If you become aware that children or young people may be engaged in sexting, seek to ensure that the behaviour ceases immediately, inform the young people involved and their parents of the legal status of the activity and refer to the Safeguarding Coordinator to assess whether it ought to be reported to the police and children's social care.

If an adult is involved in sexting with a young person, the matter must be immediately reported to the police.

If someone sends an unsolicited and unwanted sext, whatever their age, report it to the Safeguarding Coordinator in the first instance so that consideration can be given as to whether the matter should be reported to the police.

Closed Circuit TV (CCTV)

The DPA and GDPR apply to the use of CCTV where the images identify individuals. The Information Commissioner's Office has produced a Code of Practice https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf for organisations and businesses that use CCTV. The Surveillance Camera Commissioner has also produced a Code of Practice https://www.gov.uk/government/publications/surveillance-camera-code-of-practice (However, both codes require to be updated in light of the GDPR).

All churches and diocese should endeavour to comply with these codes to make sure they do not breach the DPA when setting up cameras or when using or disclosing the images recorded. The Codes of Practice covers areas such as, positioning cameras, storing and viewing the images, disclosure, retention and responsibilities. It also includes information about an individual's right to see the images, under the DPA, GDPR and the Freedom of Information Act 2000.

Live Streaming of Church Services

The live streaming of Mass and other services allows the Church to reach a congregation that is not able to attend Church in person. In addition to being able to reach a wider audience than that in a physical location, live streaming can give people support and companionship and help them feel more connected to their church community. To address potential safeguarding issues, the following steps should be taken:

- Congregations should be told in advance (notice board, announcements, pew sheets) which services are streamed and which parts of the church of building are visible on the streaming.

- Children and adults at risk should only be filmed with their consent and/or the consent of parents (for children).
- Parents should be informed in writing of the intention to stream including what will be filmed, why the filming is taking place and how it will be used. This should include any intention to retain a copy of the filming for future editing or use.
- Parents should be given the option of withholding consent to their child participating in parts of a service where they will be filmed.
- Where consent is withheld, every effort should be made for the child or adult at risk to participate and be out of the view of the cameras.
- Where a recording is made and kept, you will need to consider how it is intended to be used and the purpose; recordings will need to be stored and retained in accordance with the record retention schedule.