Guidance on Use of Technology

The Diocese of Ferns recognises the need to assess the benefits of technology and how this can be used safely and effectively in line with rules which respect the dignity and rights of all users, particularly children.

Detailed policies and procedures are provided on the use of technology including digital and online systems such as

- The Internet
- The Use of Texting and Emailing
- Photography
- CCTV and Webcams

The majority of occasions when people use mobile phones, computers or take photographs of children do not provide any cause for concern. However, there are occasions when this is not the case.

At the outset it is important to identify the risks associated with the use of technology and then to minimise the risks by putting in place measures outlined below:

Consent:

The consent of parent(s)/guardian(s) and children should always be sought prior to engaging in any activity and for the use of IT equipment such as those outlined above.

An organisation may seek overall consent from its members/group leaders or it may ask for permission for set occasions **(Media Permission Form)**

Purpose:

Guidelines should be clear as to the reason and purpose of the use of the particular form of technology:

- Provide a clear brief about what is considered appropriate in terms of content and behaviour and use of equipment;
- Provide guidance on acceptable language;
- Provide guidance on storage of information;
- Provide guidance on use of photography – if using an external photographer, ensure s/he has been vetted, has identification and does not have any unsupervised access to children or one-to-one photo sessions at events;
- Images of children should never be taken which capture them in what are commonly understood as 'non-public' activities. Children should be fully and appropriately dressed and related images should always be about the activity and not focused on any individual child;
- Images should not allow the identification of a child or their whereabouts. The full name of a child should not be used. Children in vulnerable circumstances e.g. those in care or victims of any type of abuse should not be photographed;
- Provide guidance on use of mobile phone and especially on the use of mobile phone cameras, which can be easily used for offensive actions without the subject being aware of their use. Because of this risk, the use of mobile phone cameras **should be discouraged.**

Those with responsibility for the administration of sacramental programmes within the church should:

- Address the issues of photography/videoing prior to the sacramental day and explain the policy to all families who will be attending;
- On the sacramental day the priest or deacon should remind all present of that policy and reiterate the reasons for it;
- Those present should be reminded about the rights to privacy of other children, their families and the wider community;
- Be sensitive to the fact that many parent(s)/guardian(s) are reluctant to allow the general viewing of their children or of children in their care, on social networking sites such as YouTube, Facebook and others.

Guidance on Use of the Internet

It is recognised that the Internet is valuable and widely used by all. The Diocese of Ferns has issued the following guidelines which are to be included in the Code of Behaviour for each Church activity involving children.

The following is deemed unacceptable behaviour and must be avoided in every situation:

- Visiting Internet sites that contain offensive, obscene, pornographic or illegal material;
- Using a computer to perpetrate any form of fraud or piracy;
- Using the Internet or email systems to send offensive and harassing material to others;
- Using obscene or racist language in computer assisted communications;
- Publishing defamatory or otherwise false material generated by oneself or by others through social networking;
- Introducing any form of malicious software into the used network;
- Intentionally damaging any information communication technology equipment;
- Using another user's password, or giving that password to a third party.

It is important that the following is made clear to all who use the Internet:

- All Church personnel /volunteers / group leaders must be made aware of their responsibility and sign up to appropriate use of the Internet as part of a Code of Behaviour;
- Responsibility is about safeguarding children, taking care of oneself, one's co-workers and group leaders;
- Anyone using a shared computer requires their own individual password;
- Training in appropriate and responsible Internet and computer use is imperative in order to follow best practice in all activities that concern children, co-workers and volunteers.

Guidance on Use of Texting and Email

Texting and email is a very quick and effective method of communication for those involved in Church activity. However, there are certain risks associated with its safe and appropriate use that must be managed.

The risks of text and email messaging for children and young people are:

- Inappropriate access to, use of sharing of personal details (names, numbers, email addresses);
- Unwanted contact with children/ young people by adults with bad intent, text bullying by peers etc.;
- Being sent offensive or otherwise inappropriate materials;
- Grooming for sexual abuse;
- Direct contact and actual abuse.

The risks for adults include:

- Misinterpretation of their communication with young people;
- Potential investigation (internal or by statutory agencies);
- Potential disciplinary action.

Using bulk (or bundled) text and email messaging

A way to minimise the risks above is to use bulk text messages. These are the same text or email message being sent to several young people involved with a particular activity or group. The advantage of this approach is that it presents fewer opportunities for misuse and abuse than personal, one-to-one texting or emailing arrangements between staff or volunteers and children / young people. Therefore one-to-one texting or emailing should be strongly discouraged and only occur in exceptional circumstances. The same applies to emailing young people. The following guidance is provided to minimize risk to all:

1. Consent must be obtained prior to sending young people text or email messages. For young people 15 or under, specific consent must be obtained from their parents. Guardians of younger children should be offered the option to be copied texts and emails their child will be sent. Written consent must be obtained from the guardians and young people themselves.
2. The young people's mobile phone numbers or email details should be stored in either a locked secured cabinet, or on an electronic system which is password protected, with access only available to the staff or volunteer identified to the young people and guardians as a group leader. The numbers or details should not be shared with anyone else, and should **only** be used for the purposes of the text and email messaging system regarding the Church activity.
3. All text and email messages must be sent via a bundle to a group of young people, i.e. the same standard text message being sent to every member of the group. The text and email messaging system should never be used to send text or email messages on an individual basis (i.e. to just one person);
4. All text and email messages sent must make it clear to the young people receiving it who has sent the message, rather than simply giving the mobile phone number that the system uses to send the message or the issuing email address;
5. Young people should not be given the opportunity to text or email back to the system. It should only be used as a one-way communication channel;
6. The text and email messages, which are sent, must never contain any offensive, abusive or inappropriate language;
7. When this guidance is being provided in relation to Church related activities, all of the text or email messages sent must be directly related to Church activities. The text or email messaging system and mobile phone numbers must never be used for any other reason or in any other way;
8. All of the text and email messages sent should include a sentence at the bottom, which provides young people with the opportunity to unsubscribe from receiving further text and email messages.

Guidance on Use of Photography

The use of photos on websites and in other online/hardcopy publications can pose direct and indirect risks to children and young people

Risks to Children
Even if the child's personal identity (full name, address) is kept confidential, other details accompanying the photo can make them identifiable and therefore vulnerable to individuals looking to groom children for abuse. There is also a risk that the photo itself is used inappropriately by others. Photos can easily be copied and adapted, perhaps to create images of child abuse, which can then find their way on to other websites.

How to minimise risks
- Establish the type of images that appropriately represent the activity and think carefully about any images showing children and young people on the Church website or publication;
- Never supply the full name(s) of the child or children along with the image(s);
- Only use images of children in suitable dress and focus on the activity rather than a particular child;
- Obtain permission –Guardians' and children's permission should always be sought to use an image of a young person. Guardians should be aware of the Church's policy on using children's images and of the way these represent the Church or activity. This must be recorded on a joint Consent Form for use of images of children. The child's permission must also be recorded, depending on age, to use their image. This ensures that they are aware of the way the image is to be used to represent the activity (**Template 18**).

Using photographers
Photographers are often employed by the Church for certain sacramental or Church activities.
When using a photographer it is important to do the following:
- Provide a clear brief about what is considered appropriate in terms of content and behaviour;
- Ask if the photographer has been vetted;
- Issue the photographer with identification, which must be worn at all times;
- Do not allow unsupervised access to children or one-to-one photo sessions at events;
- Do not allow photo sessions away from the event, for instance at a young person's home;
- Inform parents and children that a photographer will be in attendance and ensure they consent to both the taking and publication of films or photos.

If parents and parishioners are intending to photograph or video at an organised event, they should also be made aware of what is permitted and what is not.

Responding to concerns
Children and parents should be informed that if they have any concerns regarding inappropriate or intrusive photography, these should be reported to the Church Authority to ensure that any reported concerns are dealt with in the same way as any other child protection or child safeguarding issue.

Guidance on Use of CCTV and Webcams

The Diocese of Ferns recognises that the expanded use of CCTV and the Internet has wide implications and unless such systems are used with proper care and consideration they can give rise to concern that the individual's 'private space' is being unreasonably invaded or eroded. Section 2(1) c (iii) of The Data Protection Act requires that data are "adequate, relevant and not excessive" and fit for purpose for which they are collected.

If a Parish (data controller) is satisfied that it can justify the installation of a CCTV system, it must carefully consider what it will be used for and if these uses are deemed reasonable in the circumstances. Security of premises or other property is probably the most common use of a CCTV system and as such will typically be intended to capture images of intruders, of individuals damaging property, removing goods without permission. Using a CCTV to constantly monitor employees is highly intrusive and would need to be justified by reference to special circumstances.

Location of CCTV
The location of CCTV is a key consideration and the use of such within areas where individuals would have a reasonable expectation of privacy.
Cameras placed so as to record external areas should be positioned in such a way as to prevent or minimize recording of passers-by or of another person's private property.

Guidelines in installing CCTV camera:

- If CCTV cameras are in place it is important to have very obvious signs informing Church personnel, parishioners, volunteers and the public that this is the case;
- All uses of CCTV must be appropriate and fit for a specific purpose. As CCTV infringes the privacy of persons captured in the images there must be a genuine reason for installing such a system;
- If installing such a system the purpose for doing so must be displayed in a prominent place and preferably behind a locked notice board where it will not be damaged or removed. At a Church an obvious place would be within the porch and at all entrances.
- Images captured should be retained for a maximum of 28 days (see section 2 (1) c (iv) of Data Protection Acts). An exception for a longer duration would be where images need to be retained specifically in the context of an investigation;
- Tapes should be stored in a secure environment with a log of access to tapes kept. Access should be restricted to authorised personnel. Similar measures should be in place when using disc storage, with automatic logs of access to the images created.

Guidance on Use of Webcams

Web Broadcasting

- Cameras should be installed with due care and respect for the church building
- Cameras should only be switched on during Mass or other liturgical events and switched off at the end. There should be no live streaming of churches when there is no Mass or liturgical event taking place.

There are a number of Data Protection issues that must be met in relation to broadcasting on the net as follows:

- Recording people via a web camera and the subsequent displaying of such images over the Internet is regarded as the processing of personal data and it is imperative that it must be done with the consent of the individual;
- Camera shots (images) of the congregation should be wide shots – minimizing the possibility of easily identifying individuals with close up images;
- Signs should be placed at all entrances to the church and in other prominent locations informing those attending ceremonies within the church or visiting that web cameras are in operation;
- Parish workers, volunteers and clergy should give written consent to their image being used for web broadcasting during the course of their regular duties. Copies of this written consent should be kept in a safe place which is locked;
- Altar Servers, Ministers of the Word and Eucharistic Ministers and others taking part in liturgies (e.g. choirs and musicians) should give their consent. In the case of children written consent is required from parents/guardians;
- Service providers should be able to give regular and accurate information regarding the number of people who actually log to view. This information is important for future planning and accessing the value of web broadcasting;
- If connecting to the parish broadband ensure that the broadband package has unlimited usage for uploading or there is a risk of incurring significant costs from the provider;
- It is imperative that during broadcasting that it can be terminated to stop transmission and this should be done by accessing the control panel of the system. If this is not accessible by the priest from the altar, someone should be delegated to break transmission as required.