KANDLE
KILDARE AND LEIGHLIN DIOCESE

Diocese of Kildare & Leighlin

Safe Use of IT Policy

2026

Introduction

Children, young people and vulnerable adults are welcomed and encouraged to participate in the diocese of Kildare and Leighlin. To facilitate this, communication with children, young people, vulnerable adults, parents and carers should use the language and media with which they are familiar and comfortable. Using appropriate and safe digital media is a good way to involve children, young people and vulnerable adults in diocesan and parish activities. Such communication should have at its core, best safeguarding practice. This is achieved by ensuring, always, the appropriate use of language, images, photography, and messaging.

Children, young people and vulnerable adults must be protected from all forms of online abuse and exploitation, including such activities as online bullying, grooming, and sexting.
Complaints and/or allegations of inappropriate online communication must be taken seriously. Any concern must immediately be reported to the Designated Liaison Person (DLP) and where necessary, the Civil Authorities (An Garda Síochána / Tusla, The Child and Family Agency).

The Diocese of Kildare and Leighlin is committed to involving children, young people and vulnerable adults in developing good digital practice and will seek their views regarding safe usage in any related activity. At the same time, any activity involving under 18s requires informed parental/guardian consent. This is central to our safeguarding practice and must always be obtained whenever we engage with children and young people.

It should be noted that the age of "Digital Consent" in Ireland is sixteen (16) years of age.

Should a parish/diocesan group feel that they have exceptional cause to deviate from the policy outlined, they should discuss this matter with the DLP before taking such action.

Digital media is defined as any form of communication between two parties or more using electronic devices such as phones, computers, and tablets. (This list is not exhaustive).
Those who minister and/or work for or on behalf of the Diocese of Kildare & Leighlin, must observe appropriate professional boundaries with the children and young people they encounter through their work. This requirement applies to their use of information technology (IT), mobile phones, and social media. They should not use any of these media to initiate or maintain personal relationships with children and young people.

In particular, they must:

- **be Garda Vetted by the diocese.** This should be renewed every three years;

- attend **Diocesan Safeguarding Training**, to be renewed every three years;
- complete an **Application/ Declaration Form**;
- be given a copy of the **Adult Code of Conduct for Staff & Volunteers;**
- **report any suspicion, concern, or allegation of abuse to the DLP**;
- **be competent in the use of the technology** they use.

They should not:

- gather or retain a young person's mobile phone number (except where this is done for a specific purpose related to their work);
- provide a young person with their own personal mobile phone number or email address;
- access the internet with a young person (unless authorised to do so as part of their work);
- befriend a young person on a social media forum such as WhatsApp, Snapchat, Tiktok etc.

All forms of digital communication must have a minimum of two Administrators appointed by the parish. It is the role of these administrators to monitor all communications on the relevant platforms. Only parish devices (such as mobile phones or computers), or parish accounts (such as designated parish email), should be used to contact young people. Privately-owned devices should never be used to contact young people.

Where exceptions arise, such as trips away from home, this should be clearly communicated to parents/guardians prior to the event, and relevant consent sought.

Mobile Phones

Many children and young people have access to mobile phones. Given that mobile phone devices can perform a myriad of tasks, it is the responsibility of the youth leader/event organiser to determine and explain the level of mobile phone usage deemed appropriate.

When participating in groups with children, ensure that you have their parent/guardian's telephone contact

details and that all arrangements are made with parents/guardians.

Do not share your personal mobile phone number with children and young people. In emergency circumstances where this is unavoidable, follow this up with a telephone call to their parents/guardians to make them aware of the content. A written record should be kept of any such contact.

Communication (via email or texting) with young people under 16 years of age is not permitted.

Communication (via email or texting) with young people aged 16 to 18 years old is only permitted with prior written consent from the young person and their parents/guardians. Parents/guardians must be included in these emails and texts.

Email communication should be made using the parish/diocesan email account only. Text communication should only be made using a parish/diocesan device.

Texts or emails should be used for delivering information, a one-way communication channel. The exception to this is if a response is deemed essential. For example, a parent/guardian replying to inform a leader that a young person is unable to attend an event.

Photography and Digital Cameras

Taking photographs of children and young people is not permitted without prior signed parental/guardian consent.

Children and young people's consent should also be sought.

Photographs should only be taken by authorised personnel with a suitable reason with prearranged consent from parents/guardians and children and young people.

When using a photographer ensure that they wear identification at all times.

Do not allow the photographer unsupervised access to the children and young people.

Children and young people must not be identified in photographs.

Any photography concerns must be reported to the event organiser and DLP.

Internet Usage and Websites

Avoid participating in using the internet with children and young people with whom you are working if it is not a direct requirement for the nominated activity.

If internet usage is available as part of an activity, seek prior IT consultation to ensure that safety requirements are met.

Have a plan for responding to circumstances where unsuitable material is accessed.

Seek expert advice when considering setting up a website.

Any use of IT to access sites that are pornographic or illegal when working with children and young people is strictly prohibited.

Any concerns/allegations re: illegal or inappropriate use of IT should be reported to the DLP.

Social Media

Communication via social media platforms with young people under 16 years of age is not permitted.

The use of social media by parish groups should be for the purpose of broadcasting information about the specific parish activity involved. It should not be used as a form of social interaction between the leaders and the young people.

Any contact with young people (16 years upwards) via social media, must be done using a parish account.

Leaders should never use their own personal accounts.

All parish social media accounts must have at least two administrators.

Administrators of parish social media accounts should monitor these regularly for any traffic or comments which could be deemed offensive or inappropriate.

Never befriend young people with whom you are communicating on social media sites. This includes Facebook, Whatsapp, Twitter, Snapchat, Instagram, YouTube, TikTok. (This list is not exhaustive).

If you use social media, remember to respect the privacy of others.

Report any inappropriate material that you come across to the DLP and/or to the Civil Authorities.

Where possible, turn off private messaging on whatever platform you are using.

Live Video Platforms (Zoom, Microsoft Teams, etc.)

For the purpose of clarity, a teenager is a person aged thirteen years of age and older. Live video platforms should not be used to engage with children under the age of thirteen unless a parent/guardian is visibly present throughout the meeting.

Parishes/diocesan agencies should not use the free version of Zoom as it does not include the security measures that the subscription versions do.

Subscriptions to live video platforms, in general, should be taken out by the parish, and not by individuals. This should be managed by someone who understands the platform and who is appointed by the priest in charge.

Church personnel should NOT use a private live video platform account to contact teenagers.

If for any reason a meeting is infiltrated from the outside, that is, if somebody not invited to the meeting

appears, the meeting should be terminated immediately. The breach should be reported to the platform provider.

If the organisers feel that such a breach poses a threat of harm or abuse of the teenagers taking part, this should be reported to the Diocesan DLP. Parents/guardians should also be informed so that they can decide if they want their child to continue using the platform going forward.

Webcams and CCTV

Parishes should strive to get the best possible quote for installation and streaming costs from your webcam service provider. This should be reviewed by your parish on a regular basis. Competition between suppliers has seen a significant decrease in costs recently.
Cameras should be installed with due care and respect to church buildings. They should not be permanent fixtures; they should be easily removable without any impact on the building.

Cameras should only be switched on for the duration of Mass or other Liturgies and switched off at the end. There should be no live streaming of Churches when there is no Mass or Liturgy taking place.
There are several Data Protection issues that must be met in relation to broadcasting on the internet. 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 one of the key provisions regarding the processing of such data is that it must be done with the consent or knowledge of the individuals concerned.
Camera shots (images) of the congregation should be wide shots — minimising the possibility of easily identifying individuals with close-up images.
Signs should be placed at a range of entrances to the church and in other prominent locations informing people that web cameras are in operation.
Parish workers and members of the clergy should sign forms consenting to their image being used for web broadcasting in the course of their regular duties. Copies of consent forms should be kept on parish records.
With regard to altar servers and others taking part in Liturgies (e.g. choirs, musicians, Ministers of the Word, and Eucharistic Ministers) it is advised that consent be also obtained. In the case of children, consent by parents/guardians is required.
If you have any queries regarding the safe use of Webcams or CCTV, contact the Diocesan Data Protection Officer via email dpo@kandle.ie

Title of Policy:	**Diocese of Kildare and Leighlin - Safe Use of IT**
Date Issued:	2026
Next Review Date:	February 2029

Principal Author:	**Reviewed by:**	**In consultation with:**
Kildare and Leighlin Safeguarding Committee	Ailish Higgins, Diocesan Director of Safeguarding & DLP	Kildare and Leighlin Safeguarding Committee

Approved by:		**Date:**
Bishop Denis Nulty	+ Denis Nulty Bishop of Kildare and Leighlin	09/03/2026

Policy History

Version	**Date Approved**	**List Section numbers changed**	**Author**
1	2026	First edition	Kildare and Leighlin Safeguarding Committee