**GDPR Guidelines for Parishes using Webcams**

**Webcam Guidelines for Live Streaming of Liturgies (no recording)**

Web cams stream images of identifiable individuals over the internet via a web camera and no recordings take place. Their use, however is regarded as the processing of personal data and is subject to the GDPR. One of the key provisions regarding the processing of personal data is that it should be done with the consent or knowledge of the individuals concerned. The following guidelines will help you with GDPR compliance;

1. Place notices in your newsletter that a web cam is in operation and inform parishioners of the liturgy schedule that will be live streamed on the internet.
2. Place signage at each entrance to the church and in other prominent locations informing people that web cameras are in operation. Also inform parishioners of the liturgy schedule that will be live streamed.
3. A sign should also be placed in the Sacristy to inform visiting priests and others of web cam use
4. Cameras should only be switched on for the duration of Mass or Liturgy and switched off at the end.
5. During any broadcast it should be possible to stop transmission, if necessary, by quickly accessing the control panel of the system. If this cannot be done by the priest from near the altar, someone should be delegated to break transmission when necessary.
6. Camera images of the congregation should be wide shots minimising the possibility of easily identifying individuals with close up shots. This is particularly relevant for funeral ceremonies.
7. No live streaming should take place once the ceremonies have finished.
8. With regard to altar servers and others children taking part in Liturgies it is advised that consent is obtained from their parents/guardians. The parental/guardian consent given for the use of media/webcams in the Safeguarding Forms (Alter Server Applications Form or Child & Parent/Guardian Joint Activity and Media Consent Form) will be sufficient for parental/guardian consent.
9. Cameras should be installed with due care and respect in church buildings. They should not be permanent fixtures. They should be easily removable without any impact on the building.
10. The installer and operator of the web cam system is known as a Service Provider or Data Processor (third-party) under the GDPR. You are required to have a Service Provider Agreement (see F008-1) in place with them. This Agreement details what you allow them to do with your data; what security standards should be in place and what verification procedures may apply. It ensures that any sub-contractors they employ, e.g. maintenance engineers, follows this agreement. The parish will be open to data breaches if the Service Provider or one of their sub-contractors can distribute or remove personal data in the form of images without following your agreement*.*
11. Service providers may be able to access the web cams remotely and they may be able to give regular, accurate information regarding the number of people who actually log on to view Liturgies from your parish in order for you to assess the value of web broadcasting. ***This will have to be included as part of your Privacy Statement as people are entitled to know this information.***

**Webcam Guidelines for Recording Liturgies and/or Recording for Security Purposes.**

1. If you also use your webcam to record, this is considered processing of data and therefore subject to the GDPR. Prominent notices should be placed in the newsletter and on church entrances, informing parishioners that recording is taking place for a particular service or liturgy with dates and times given.
2. If your webcam is recording for security purposes, ensure that your cctv signs are visible.
3. Any act of storage or access is considered processing and it is imperative that the Parish and [security operators uphold the confidentiality and integrity of any footage](https://netwatchsystem.com/blog/cctv-gdpr-data-protection/).
4. Back-up tapes/discs should be stored in a secure environment with an access log maintained (similar to cctv). Access should be restricted to authorised personnel only. If back-ups are being stored on the Cloud then you need to know where the Cloud data centre is based. If it is in the European Economic Area (EEA) there is no problem but if it is located outside of the EEA then you will have to get your system operators to move it.

