Standard 1

Creating and Maintaining Safe Environments

Guidance for Indicator 1.9

Guidance on Use of CCTV and Webcams

The increasing 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. Each Church body must have an appropriate data protection policy in place that covers the use of webcam and CCTV images.

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 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, or of individuals damaging property or 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. The retail sector is one example where there is evidence to suggest that money or goods could be removed without authorisation.

The location of CCTV is a key consideration, and its use within areas where individuals would have a reasonable expectation of privacy, e.g. toilets and changing rooms, would be difficult to justify.

Cameras placed so as to record external areas should be positioned in such a way as to prevent or minimise recording of passers-by, or of another person's private property.

Having acknowledged the positive and sometimes negative aspect of CCTV, each Church body should draw up a policy and guidelines in order to maximise the benefit of such installations and minimise the possibility of a person's privacy being infringed.

The following should be considered:

- 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 noticeboard where it will not be damaged or removed. In a church, an obvious place would be within the porch and at all entrances;

- Images captured should be retained for a maximum of twenty-eight days (see Section 2 [1] c [iv] of the Data Protection Act). 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, along with a log of access to tapes. Access should be restricted to authorised personnel. Similar measures should be in place when using disc storage, with the creation of automatic logs of access to the images.

Web Broadcasting

There are a number of data protection issues that must be met in relation to broadcasting on the internet. The policy should be reflective of these:

- Recording people via a web camera, and the subsequent displaying of such images over the internet, is regarded as the processing of personal data. It is imperative that it must be done with the consent of the individual;
- 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 all entrances to the church and in other prominent locations, informing those attending ceremonies or visiting the church that web cameras are in operation;
- If the Church activity being recorded involves children (for example as altar servers, ministers of the word, choirs etc.) then their written consent and that of their parents/guardians is required.
- Service providers should be able to give regular and accurate information regarding the number of people who actually log in online to view. This information is important for future planning and assessing the value of web broadcasting;
- If connecting to the parish broadband, ensure that the broadband package has unlimited usage for uploading, or else there is a risk of incurring significant costs from the provider;
- It is imperative that live broadcasts can be terminated to stop transmission. 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 if required.