Midleton Community Forum clg, TA Midleton FRC
GDPR/Data Protection Policy

Policy

Midleton Family Resource Centre is committed to a policy of protecting the rights and privacy of individuals in accordance with the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. For administrative purposes (e.g. to pay staff, to administer programmes, to record progress and to comply with legal obligations to funding bodies and government), the Centre needs to process personal data about its staff, volunteers and other individuals with whom it has dealings. To comply with the law, personal data must be collected and used
fairly, stored safely and securely and not disclosed to any third party unlawfully.

Individuals' Responsibilities

Any member of the Centre who is involved in the collection, storage or processing of personal data has responsibilities under the legislation and should make sure to:

- Obtain and process personal data fairly
- Keep such data only for explicit and lawful purposes
- Disclose such data only in ways compatible with these purposes
- Keep such data safe and secure
- Keep such data accurate, complete and up-to-date
- Ensure that such data are adequate, relevant and not excessive
- Retain such data for no longer than is necessary for the explicit purpose
- Give, on request, a copy of the data to the individual to whom they relate such a request is known as an Access Request.

Individual Rights

The individuals for whom the Centre stores personal data have the following rights:

- To have their personal data obtained and processed fairly, kept securely and not illegitimately disclosed to others

- To be informed of the identity of the Data Controller and of the purpose for which the information is held
- To get a copy of their personal data
- To have their personal data corrected or deleted if inaccurate
- To prevent their personal data from being used for certain purposes: e.g. blocked for research purposes
- Under Employment Rights, not to be forced to disclose information to a prospective employer. No one can force another person to make an access request, or reveal the results of an access request, as a condition of recruitment, employment or provision of a service. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.

It should be noted that under the Freedom of Information Act (1997 and 2003) records containing personal information may be released to a third party, where the public interest so requires.

Principles of the Acts

The Centre will administer its responsibilities under the legislation in accordance with the eight stated data protection principles outlined in the Act as follows:

1. *Obtain and process information fairly*
   The Centre will obtain and process personal data fairly and in accordance with the fulfillment of its functions
2. *Keep data only for one or more specified, explicit and lawful purposes*
   The Centre will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes
3. *Use and disclose data only in ways compatible with these purposes*
   The Centre will only disclose personal data that is necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data

4. *Keep data safe and secure*

   The Centre will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The Centre is aware that high standards of security are essential for all personal data

5. *Keep data accurate, complete and up-to-date*

   The Centre will have procedures that are adequate to ensure high levels of data accuracy and will examine the general requirement to keep personal data up-to-date. Appropriate procedures will be put in place to assist staff in keeping data up-to-date

6. *Ensure that data are adequate, relevant and not excessive*

   Personal data held by the Centre will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept

7. *Retain data for no longer than is necessary for the purpose or purposes for which they are kept*

   The centre will implement a policy on retention periods for personal data

8. *Give a copy of his/her personal data to that individual, on request*

   The Centre will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

Roles/Responsibilities

The Family Resource Centre has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees of the Centre who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation. The Centre will provide support, assistance, advice and training as required in order to ensure that it is in full compliance with the legislation.

Procedures and Guidelines

This policy supports the provision of a structure to assist the Centre's compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

Review

This Policy will be reviewed regularly in light of any legislative or other relevant indicators.

Data Protection and CCTV

The use of CCTV systems has greatly expanded in recent years. So has the sophistication of such systems. Systems now on the market have the capacity to recognise faces. They may also be capable of recording both images and sounds.

The expanded use of CCTV systems has society-wide implications. 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 eroded.

Recognisable images captured by CCTV systems are personal data". They are therefore subject to the provisions of the Data Protection Acts.

A data controller needs to be able to justify the obtaining and use of personal data by means of a CCTV system. A system used to control the perimeter of a building for security purposes will usually be easy to justify. The use of CCTV systems in other circumstances - for example, to constantly monitor employees, customers or students - can be more difficult to justify and could involve a breach of the Data Protection Acts.

Proportionality - is a CCTV system justified?

Section 2(1)(c)(iii) of the Acts require that data are "adequate, relevant and not excessive" for the purpose for which they are collected. This means that an organisation must be able to demonstrate that the serious step involved in installing a system that collects personal data on a continuous basis is justified. Before proceeding with such a system, it should also be certain that it can meet its obligations to provide data subjects, on request, with copies of images captured by the system.

Proportionality - what will the system be used for?

If a data controller is satisfied that it can justify installing a CCTV system, it must consider

what it will be used for and if these uses are reasonable in the circumstances.

Security of premises or other property is probably the most common use of a CCTV system. Such a system will typically be intended to capture images of intruders or of individuals damaging property or removing goods without authorisation. Such uses are more likely to meet the test of proportionality.

Other uses may fail the test of proportionality. For example, using a CCTV system to constantly monitor employees is highly intrusive and would need to be justified by reference to special circumstances. If the monitoring is for health and safety reasons, a data controller would need to demonstrate that the installation of CCTV was proportionate in addressing health and safety issues that had arisen prior to the installation of the system.

Proportionality - what images will be captured?

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Toilets and rest rooms are an obvious example. To justify use in such an area, a data controller would have to demonstrate that a pattern of security breaches had occurred in the area prior to the installation of the system such as would warrant constant electronic surveillance. Where such use can be justified, the CCTV cameras should never be capable of capturing images from cubicles or urinal areas.

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.

Transparency

Section 2D of the Acts requires that certain essential information is supplied to a data subject before any personal data are recorded. This information includes:

the identity of the data controller;
the purposes for which data are processed;
any third parties to whom the data may be supplied.

This can usually be achieved by placing easily- read and well-lit signs in prominent positions. A sign at all entrances will normally suffice.

If the identity of the data controller and the usual purpose for processing - security - is obvious, all that need be placed on the sign is a statement that CCTV is in operation as well as a contact (such as a phone number) for persons wishing to discuss this processing. This contact can be for either the security company operating the cameras or the owner of the premises.

If the purpose or purposes is not obvious, there is a duty on the data controller to make this clear. A CCTV camera in a premises is often assumed to be used for security

purposes. Use for monitoring staff performance or conduct is not an obvious purpose and staff must be informed before any data are recorded for this purpose. Similarly, if the purpose of CCTV is also for health and safety reasons, this should be clearly stated and made known.

Storage and retention.

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which they were obtained. A data controller needs to be able to justify this retention period. For a normal security system, it would be difficult to justify retention beyond a month, except where the images identify an issue - such as a break-in or theft - and is retained specifically in the context of an investigation of that issue.

The storage medium should be stored in a secure environment with a log of access kept. Access should be restricted to authorised personnel.

Supply of CCTV Images to An Garda Síochána

If the Gardaí want CCTV images for a specific investigation, it is up to the data controller to satisfy himself that there is a genuine investigation underway. For practical purposes, a phone call to the requesting Garda's station may be sufficient, provided that you speak to a member in the District Office, the station sergeant or a higher ranking officer, as all may be assumed to be acting with the authority of a District/Divisional officer in confirming that an investigation is authorised.

Access Requests

1. Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage. To exercise that right, a person must make an application in writing.

2. When making an access request for CCTV footage, the requester should provide the data controller with a reasonable indication of the timeframe of the recording being sought - i.e. they should provide details of the approximate time and the specific date(s) on which their image was recorded. For example, it would not suffice for a requester to make a very general request saying that they want a copy of all CCTV footage held on them. Instead, it is necessary to specify that they are seeking a copy of all CCTV footage in relation to them which was recorded on a specific date between certain hours at a named location. Obviously, if the recording no longer exists on the date on which the data controller receives the access request, it will not be possible to get access to a copy. Requesters should be aware that CCTV footage is usually deleted within one month of being recorded.

3. For the data controller's part, the obligation in responding to the access request is to provide a copy of the requester's personal information. This normally involves providing a copy of the footage in video format. In circumstances where the footage is technically incapable of being copied to another device, or in other exceptional circumstances, it is acceptable to provide stills as an alternative to video footage. Where stills are supplied, it would be necessary to supply a still for every second of the

recording in which the requester's image appears in order to comply with the obligation to supply a copy of all personal data held.

4. Where images of parties other than the requesting data subject appear on the CCTV footage the onus lies on the data controller to pixilate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requestor. Alternatively, the data controller may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester

5. Where a data controller chooses to use technology to process personal data, such as a CCTV system to capture and record images of living individuals, they are obliged to shoulder the data protection obligations which the law places on them for such data processing. In the matter of access requests for CCTV footage, data controllers are obliged to comply fully with such requests. Claims by a data controller that they are unable to produce copies of footage or that stills cannot be produced from the footage are unacceptable excuses in the context of dealing with an access request. In short, where a data controller uses a CCTV system to process personal data, its takes on and is obliged to comply with all associated data protection obligations.

Covert surveillance.

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies that a written specific policy be put in place detailing the purpose, justification, procedure, measures and safeguards that will be implemented with the final objective being, an actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a consequence of an alleged committal of a criminal offence(s).

Covert surveillance must be focused and of short duration. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.

If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy.

Responsibilities of security companies.

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors". As data processors, they operate under the instruction of data controllers (their clients). Sections 2(2) and 2C of the Data Protection Acts place a number of obligations on data processors.

These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all

unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.

Staff of the security company must be made aware of their obligations relating to the security of data.

Clients of the security company should have a contract in place which details what the security company may do with the data; what security standards should be in place and what verification procedures may apply.

Furthermore, section 16 of the Data Protection Acts 1988 & 2003 requires that certain data processors must have an entry in the public register maintained by the Data Protection Commissioner. For further information, please refer to our Guidance notes on Registration. Those parties who are required to be registered and process data whilst not registered are committing a criminal offence and may face prosecution by this office. (This provision may only apply where the data controller can identify the persons whose images are captured.)

Domestic use of CCTV systems.

The processing of personal data kept by an individual and concerned solely with the management of his/her personal, family or household affairs or kept by an individual for recreational purposes is exempt from the provisions of the Acts. This exemption would generally apply to the use of CCTVs in a domestic environment. However, the exemption may not apply if the occupant works from home. [Where the exemption does apply, a person who objects to the use of a CCTV system - for example, a neighbour who objects to images of her/his property being recorded - may be able to take a civil legal action based on the Constitutional and Common Law right to privacy.]