**RATIONALE**

LEAP exists to provide effective and innovative housing and support services to vulnerable young people at risk.

This policy and the procedures that it underpins apply to all staff, including senior managers and the board of trustees, paid staff, volunteers and sessional workers, agency staff, students and anyone working on behalf of LEAP

**VISION**

We recognise long-term success depends on young people living in a safe, supported, respectful and learning environment; having a sense of safety and the right to live in their home without threat of harm from others and without the fear of crime.

**PRINCIPLES**

The system is owned and operated by LEAP Ltd and is sited at the schemes listed in Appendix A. LEAP is therefore legally responsible for the system and as such is the Data Controller for the purposes of the Data Protection Act 1998. The Chief Executive has delegated responsibility for ensuring the day-to-day compliance with this policy.

All recorded material is owned by and the copyright of LEAP. This policy and procedure has been agreed with the Board of Directors and Trustees of the charity and has been prepared for the guidance of all users of the system, including the management and staff of LEAP. LEAP is committed to compliance with all aspects of this CCTV policy.

The CCTV system is operational 24 hours a day, 365 days a year.

LEAP’s CCTV systems will operate fairly, within the law, and only for the purposes for which they were established or which are subsequently agreed in accordance with this policy.

The services will be delivered and operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their homes in accordance with the provisions of the Human Rights Act 1998.

The public interest in the operation of the services will be recognised by ensuring the security and integrity of operational procedures.

Throughout this policy it is intended, as far as reasonably possible, to offer a balance between the objectives of the CCTV systems in place and the need to safeguard the individuals right to privacy. Throughout the policy every effort has been made to indicate that a formal structure has been put in place (including a complaints procedure), by which it should be identified that the services are not only accountable, but are seen to be accountable.

The main purposes of the scheme are:

* A reduction in the fear of crime and reassurance of LEAP clients.
* To help secure a safer environment for those people who live, visit and work at LEAP premises.
* The detection, deterrence and prevention of crime, such as:
* Helping to identify and prosecute offenders;
* Providing the Police with evidence to take criminal action in the courts;
* Assisting in the delivery of LEAP services by reducing risk to LEAP staff and clients.

The key objective of the service is as follows:

* LEAP will use the system to detect, prevent or reduce the incidence of property crime and offences against the person.
* It will also be used to ensure that vulnerable young people are safeguarded against abuse.

As the services will only be used as detailed above, processing the information collected will be solely as defined by paragraph 5(d) of Schedule 2 of the Data Protection Act 1998.

The ultimate aim of the service is to make LEAP accommodation a desirable and safe place to live and work.

It is important to emphasise that the CCTV systems used are not "spy systems". They are intended to detect crime and the criminals involved and lead to successful prosecution. There will be no deliberate monitoring of people, or employees of LEAP, carrying out their legitimate business. However, random monitoring by management will take place in order to ensure that policies and procedures are carried out appropriately and that staff and clients are able to work and reside safely within LEAP accommodation facilities.

When agencies with prosecution powers such as Police, Health and Safety Executive etc. request evidential material it will be provided upon the approval of Senior Management.

The policy will be supplemented by procedure giving detailed instructions on all aspects of operation. The procedure will be based on the policy to ensure that the principals and purposes on which it is based are realised.

**Data Protection Act 1998**

The CCTV service is registered with the office of the Data Protection Commissioner, with LEAP being nominated as the Data Controller.

All data will be processed in accordance with the principles of the Data Protection Act 1998 which, in summarised form, includes, but is not limited to:

* All personal data will be obtained and processed fairly and lawfully.
* Personal data will be held only for the purposes specified.
* Personal data will be used only for the purposes, and disclosed only to the people, shown within this policy.
* Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which it is held.
* Personal data will be held for no longer than is necessary.
* Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

Above all the systems will comply with the Information Commissioners CCTV Code of Practice revised edition 2008.

**Regulation of Investigatory Powers Act 2000**

The Regulation of Investigatory Powers Act 2000 came into force in October 2000 to regulate the use of relevant investigatory powers in accordance with human rights. The Act regulates both “Directed” and “Intrusive” surveillance. LEAP is not authorised to undertake intrusive surveillance.

With regard to “Directed” surveillance, S.26 (2) defines this as a pre-planned activity which is:

* “covert surveillance that is undertaken in relation to a specific investigation or

a specific operation which is likely to result in the obtaining of private information about a person”.

On occasions LEAP will use the CCTV systems to undertake “Directed” surveillance providing the purpose of such surveillance is compatible with the provisions contained within the Act. It is anticipated that the majority of such surveillance will be:

* For the purpose of preventing or detecting crime or preventing disorder
* In the interests of public safety
* For the purpose of protecting clients, visitors and staff

All occasions of “Directed” surveillance must be authorised by the Senior Management.

**Human Rights Act 1998**

* The systems will be operated with due regard to the Human Rights Act 1998 and in particular the provisions of Article 8, conveying on an individual the qualified right to respect for his or her private and family life.
* No interest will be shown in private property and cameras will not look into such areas. In addition the use of cameras elsewhere will be proportionate to the objectives detailed in this policy.
* LEAP staff will have clear guidelines and any inadvertent contraventions will be recorded and the reasons for the occurrence given. The scheme will be managed and audited to ensure that individuals’ privacy is not breached.

The day-to-day management of the cameras will be the responsibility of the LEAP support staff who will report to a member of the management team.

Only LEAP staff will have access to the office where the cameras are viewed. Designated LEAP staff will also have access to all recorded material retained, providing such access is in accordance with both the objectives and purposes of the scheme and is authorised by the management team. Such staff are outlined in Appendix B of this policy and will at all times have due regard to their responsibilities under the Data Protection Act 1998 and Human Rights Act 1998.

**Accountability**

Copies of the policy must be made available to clients on request.

All reports on the system will be made to the Board of Directors and Trustees of the charity for their approval.

**Public Information**

* Cameras should not be hidden but should as far as is consistent with the purposes of the schemes be placed in public view.
* Clearly visible signs stating that CCTV cameras are operating will be displayed at the perimeter of the scheme and at other key points. The signs will inform the public who operates the cameras and allow people entering the area to make a reasonable approximation of the area covered by the scheme.
* There is no sound recording undertaken from any part of the system.
* The policy will be made available for inspection on the LEAP website and on request.

**Assessment of the CCTV and Policy**

Effective evaluation of the CCTV is essential to identify whether the purposes of the systems are being complied with, and whether key objectives are being achieved.

It is necessary to monitor compliance with the policy and operational guidelines. LEAP staff will be required to read the policy whenever a review takes place. When a new person is employed prior to having access to the CCTV system they must read this policy.

The management team will be responsible for the day-to-day monitoring of the scheme and compliance with the policy.

An audit of the system and compliance testing will be carried out at least annually to evidence good practice. The Chief Executive of LEAP who is not involved in the day to-day management of the system will carry this out.

The audit will include an examination of the following:

* Procedural checks and the maintenance of the security of the system
* Procedural checks on the management and operational arrangements for the system
* Compliance with data protection and Human Rights requirements
* Assurances that there are no infringements of civil liberty

**Staff**

All LEAP staff with access to the CCTV system will be subject to disciplinary procedures for breaches of confidentiality. Non-compliance with the policy will be treated as gross misconduct within the Disciplinary Code. All staff will be subject to a Disclosure and Barring Service (DBS) in line with LEAP Recruitment Policy.

**Complaints and Appeals**

Any complaints relating to the use of the CCTV system will be dealt with using the LEAP Complaints Procedure.

LEAP clients who are issued with sanctions as a result of evidence found on CCTV system can use the LEAP appeals system.

**Breaches of the Policy**

The responsibility for the policy and for security rests with the management team.

Any breaches of the policy and security will be the subject of proper investigation by the Chief Executive. Where a serious breach occurs the Chief Executive will report the matter to the Board.

**Control and Operation of Cameras and Recording Equipment**

Information recorded should be accurate, relevant and not exceed that necessary to fulfill the purpose of the scheme.

All cameras will be properly maintained and serviced to ensure clear images are recorded.

Only staff that have been authorised to use the equipment shall have access to operating the controls and recording equipment as outlined in Appendix B of this policy.

All use of the cameras shall accord with the purpose statement and key objectives of the scheme.

Cameras will not look into private property.

**Release of Information to Police and other Enforcement Bodies**

It is probable that the Police may ask to view a video recording(s) to seek supporting evidence relating to a crime. Such a request will be authorised by Senior Management upon the specific reason/purpose of the request. That request will be logged.

Recorded material will only be used for the purposes defined in this policy.

In all cases the reviewing of evidence must be carried out under the supervision of a member of the management team.

Requests by other bodies, with statutory enforcement powers, to access evidence will only be granted if an adequate justification with regard to reason and duration is demonstrated at the time of request. Senior management must approve all such requests.

**Release of Information in response to Data Subject Access Requests**

It is important that access to, and disclosure of, the images recorded by the CCTV is restricted and carefully controlled, not only to ensure that the rights of the individual are preserved, but also to ensure that the chain of evidence remains intact should images be required for evidential purposes. This policy conforms to the Second and Seventh Data Protection Principles and so copies of images may only be released for reasons which are compatible with the purposes of the CCTV system.

The right to access material by data subjects is provided in Section 7 of the Data Protection Act 1998. Any person therefore wishing to access personal data that may be recorded will be provided with a standard subject access request form. The form will request sufficient information to allow a search to be made. Such information will include the time, date and place and in addition a recent photograph must also be supplied by the individual making the request in order for the correct images to be located. The maximum search fee allowed under the Act will be required for each search requested.

In accordance with the provisions of the above Act, all requests will be responded to within 40 days of receiving the required search fee and information.

It must be noted that only images of the individual making the request will be released. No third party details will be disclosed and so such images will be blurred or otherwise disguised.

If it is decided that information cannot be provided to an individual making a data subject access request, then a written response will be provided within 21 days of receiving the request, setting out the decision and the reasons for such a decision.

**Release of Information to Third Parties**

Access to recorded images is restricted to staff that need to have access in order to achieve the purposes of the CCTV system in accordance with Appendix B of this policy.

Release of information to the media will only be where it is decided that the publics’ assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. This decision will be taken by the Chief Executive in consultation with the police and will have due regard to the wishes of the victim.

Recorded images will not be made more widely available and will not be made routinely available to the media. No recorded material will be sold or used for commercial purposes or the provision of entertainment.

**General Evidential Management**

Evidence will be presented in a digital format on a digital versatile disc (DVD). The evidence and statements will be contained in sealed evidence bags by the collecting police officer who will sign for the evidence.

In accordance with Home Office and Data Protection Commissioner Recommendations, recordings will be kept for up to a maximum of 31 days.

If evidence is not collected within 31 days of the copy date the evidence will be destroyed.

**Photographs**

Photographs from digital playback should only be used to assist in the identification of incidents.

Photographs will be supplied to Police on formal request in the same way as that for video evidence.

If the Police require a photograph then a duplicate will be made and retained in the LEAP office. A separate log will be maintained of all photographs produced which will include name of member of staff on duty, Police Officer (if applicable), time/date when photograph made, number of copies, details of the incident, and, if a copy is handed to the Police, the date/time when it was handed over.

All photographs will remain the property of LEAP.

Where photographs are not subject to Police action they shall be destroyed after 31 days.

**Police Use of the System**

The Police have no direct control of the system.

In circumstances when problems are anticipated during any part of a shift, arrangements may be made for a Police Officer to be present to view the CCTV for liaison purposes. This will normally apply for the duration of the incident and will be subject to authorisation from the Senior Management Team.

**PROCEDURE**

This procedure forms part of the CCTV policy.

LEAP’s CCTV system will operate fairly, within the law, and only for the purposes for which they were established or which are subsequently agreed in accordance with the policy.

The ultimate aim of the service is to make LEAP’s accommodation a desirable and safe place to live and work. It is important to emphasise that the CCTV systems used are not "spy systems".

Monitoring of people or employees of LEAP will only be undertaken as a means of ensuring that LEAP is a safe place to work and live rather than the monitoring of staff and clients carrying out their legitimate business. Senior Management will carry out random weekly checks of cameras selecting random dates and times. A log of all viewing will be recorded and kept safe.

All occasions of “Directed” surveillance must be authorised by a senior manager.

The day-to-day management of the cameras will be the responsibility of the LEAP support staff who report to a member of the management team.

Access to the office where the monitors are located is outlined in Appendix B of this policy. Such staff will at all times have due regard to their responsibilities under the Data Protection Act 1998 and Human Rights Act 1998. If a client visits the office they must be supervised at all times and under no circumstances should they be allowed to view or operate the CCTV system. All visitors to the office, including Clients, will be required to sign in.

The senior management team will be responsible for the day-to-day monitoring of the scheme and compliance with the policy.

All LEAP staff with access to the CCTV system will be subject to disciplinary procedures for breaches of confidentiality. Non-compliance with the policy will be treated as gross misconduct within the Disciplinary Code.

All cameras will be properly maintained and serviced to ensure clear images are recorded.

If a request is made by the Police to view a recording(s) to seek supporting evidence relating to a crime, such a request must be authorised by the management team. That request will be logged.

Access to recorded images is restricted to staff that need to have access in order to achieve the purposes of the CCTV system as defined in Appendix B of this policy.

Incidents occurring on or around the premises for example: damage, neighbour complaints, incidents reported by other clients etc. may be corroborated by inspecting the recorded material. As much information as possible with regard to date, time, descriptions of persons involved etc. should be gathered to ensure that the incident is investigated with due care and attention paid to Data Protection and Human Rights. All such inspections should be carried out by a member of the management team, logged and accompanied by an incident report.

In circumstances when problems are anticipated during any part of a shift, arrangements may be made for a Police Officer to be present to view the CCTV for liaison purposes. This will normally apply for the duration of the incident and will be subject to authorisation by the senior management team.

Recorded material must not be sold or used for commercial purposes or the provision of entertainment.

Recorded data will be destroyed after a period of 31 days.

All staff will be trained in the use of the CCTV system and will be required to sign to say they have received training and have read the policy and procedure.

**LINKS WITH OTHER LEAP POLICIES**

* Information Management

**PARTICIPATION & CONSULTATION PROCESS**

* Awareness raising programmes
* Survey/questionnaires distributed to staff and clients
* LEAP Participation Group
* Seeking the views of Stakeholders
* Monitoring evaluation and review

**RESPONSIBILITIES OF ALL STAKEHOLDERS.**

**The Responsibilities of Staff**

Our staff will:

* Operate the CCTV equipment in line with this policy to ensure that there is no infringement of privacy and that it is used only to ensure the safety of clients and staff and for the prevention and detection of crime

**The Responsibilities of Clients**

We expect our clients to:

* Ensure that they do not tamper with CCTV equipment as in order to keep them safe it is important that the equipment is operational at all times

**The Responsibilities of All**

Everyone should:

* Work towards ensuring that LEAP is a safe place to live and work

**CONTINUOUS PROFESSIONAL DEVELOPMENT OF STAFF**

* LEAP is committed to training its staff to the highest standards. This is through internal and external training, through team meetings and supervision.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of policy:** | **Author of review /revision** | **Date approved** | **Approved By** | **Next revision/ revision date:** |
| **CCTV** | Kim Bescoby | 31.01.18 | Full Board | January 2021 |

**Document Control**

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes made |
| Version 1 | April 2017 |  |
| Version 2 | January 2018 | Changes to Appendix A and B only |