COLEHILL PARISH COUNCIL

Closed Circuit Television System
Code of Practice

Document approved by resolution of the Parish Council on the 12 April 2016

Code of Practice for the Operation of the

Colehill Parish Council

Closed Circuit Television System

1 Introduction and Objectives

1.1 Introduction

Colehill Parish Council CCTV Surveillance System comprises of four external/internal cameras located in a cabinet at the Co-op, Middlehill Road. The camera has fixed views of:

- towards Middlehill Road
- the green opposite the Co-op
- the Wimborne Road/Smugglers Lane junction
- the Co-op car park

Images are stored on the system and can be accessed on site by the Contractor.

The Colehill Parish Council CCTV Surveillance System has been notified to the Information Commissioner. The Council's notification for the purposes of the Data Protection Act 1998 can be viewed on the Information Commissioner's website at: https://ico.org.uk/ESDWebPages/DoSearch

1.2 Definitions

The Code means this Code of Practice.

The Council means Colehill Parish Council.

The Data Controller means Colehill Parish Council.

The Owner means Colehill Parish Council.

The System means the Colehill Parish Council CCTV Surveillance System.

The System Manager means The Clerk to the Council.

The Contractor means Security Solutions.

Details of key personnel, responsibilities and contact points are shown in Appendix A.

References to any act, order, regulation or other similar instrument shall mean a reference to that act, order, regulation or instrument as subsequently amended, re-enacted or superseded.

1.3 Council statement in respect of The Human Rights Act 1998

1.3.1 The Council recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998. The Council considers that the use of the System is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.3.2 Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by the Council in their duty under the Crime and Disorder Act 1998.

1.3.3 The Council recognises that operation of the System may be considered to infringe on the privacy of individuals. The Council acknowledges its responsibility to ensure that the System should always comply with all relevant legislation, to ensure its legality and legitimacy. The System shall only be used as a proportionate response to identified problems and it will only be used in so far as it is necessary in a democratic society, in the interests of national security, public safety, for the prevention and detection of crime or disorder and for the protection of the rights and freedoms of others.

1.3.4 The Code and observance of the operational procedures shall ensure that evidence is secured, retained and made available as required to ensure that there is absolute respect for everyone's right to a fair trial.

1.3.5 The System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any grounds such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status and age.

1.4 Objectives of the System

1.4.1 The current priorities, as determined by the Owners, which form the lawful basis for the processing of data are:

- To help deter anti-social behaviour.
- Reduce the fear of crime and anti-social behaviour.
- To secure evidential quality images / material and store it securely
- To provide evidence to support prosecutions
- To protect staff and contractors carrying out their legitimate duties

2 Statement of Purposes and Principles

2.1 Purpose

2.1.1 This section states the intention of the Council, to support the objectives of the

System and outlines how it is intended to do so.

2.1.2 The purpose of the System and the process adopted in determining the reasons for implementing the System are as previously defined for achieving the objectives detailed within Section 1.

2.2 General Principles of Operation

2.2.1 The System will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

2.2.2 The System shall be operated in accordance with the Data Protection Act 1998 at all times.

2.2.3 The System shall be operated fairly, within the law and only for the purposes for which it was established and identified within the Code, or which are subsequently agreed in accordance with the Code.

2.2.4 The System shall be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home.

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

2.2.6 The Code is intended, as far as reasonably possible, to balance the objectives of the System with the need to safeguard the individual's rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

2.2.7 Participation in the System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with the Code and to be accountable under it.

2.3 Copyright

2.3.1 Copyright and ownership of all material recorded by virtue of the System will remain with the Data Controller.

2.4 Cameras and Area Coverage

2.4.1 The area covered by the System to which the Code refers are the public areas at the Co-op, Middlehill Road:

- towards Middlehill Road
- the green opposite the Co-op
- Wimborne Road/Smugglers Lane junction
- Co-op car park

2.4.2 The location of the cameras are not intended to be covert. The cameras will not be concealed from the view of any person likely to be within the field of view of the cameras.

2.5 Monitoring and Recording Facilities

2.5.1 The System is monitored on a quarterly basis by the Contractor. The System has the capability of recording all cameras simultaneously throughout every 24-hour period.

2.5.2 The Contractor is able to view images from the cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data in accordance with the Code. All viewing and recording equipment shall only be operated by authorised users.

2.6 Human Resources

2.6.1 Unauthorised persons shall not have access to the System without an authorised member of staff being present. All persons must be made aware of the confidentiality and data protection issues when viewing images.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, whether recorded digitally, in analogue format or as hard copy video print, will be processed and handled strictly in accordance with the Code. Release of recorded data to third parties will be in accordance with the Data Protection Act 1998.

2.8 Changes to the Code

2.8.1 Any major change to the Code which would significantly impact upon the Code or upon the operation of the System, will take place only after consultation with, and upon the agreement of the Council.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public at large may have become accustomed to being watched, those who do express concern do so mainly over matters pertaining to the processing of the information (Data), i.e. what happens to the material obtained.

3.1.2 All Data obtained by virtue of the System shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the System. Personal data shall be processed with due consideration to a persons' right to respect for his or her private and family life and their home.

3.1.3 The processing, storage and security of the Data will be in accordance with the requirements of the Data Protection Act 1998.

3.2 Data Protection Legislation

3.2.1 The operation of the System has been notified to the Information Commissioner in accordance with current Data Protection legislation.

3.2.2 The Data Controller for the System is the Colehill Parish Council but day-to-day responsibility for the data will be devolved to the System Manager.

3.2.3 All Data will be processed in accordance with the Data Protection Principles at Part 1 of Schedule 1 of the Data Protection Act 1998:

i) All Personal Data will be obtained and processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive Personal Data, at least one of the conditions in schedule 3 is also met.

ii) Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

iii) Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

iv) Personal Data shall be accurate and where necessary, kept up to date.

v) Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

vi) Personal Data shall be processed in accordance with the rights of the data subjects under this Act.

vii) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data via the use of a log book, kept in both electronic and paper format.

viii) Personal Data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data.

3.3 Request for Information (Subject Access)

3.3.1 Any request under Section 7 of the Data Protection Act 1998 for the disclosure of Personal Data that may have been recorded by the System, will be directed in the first instance to the System Manager.

3.3.2 If the request cannot be complied with, without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

3.3.3 If permission cannot be obtained from identifiable other parties, then digital pixilation may be considered subject to reasonable cost.

3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. Data subject access forms can be found at Appendix E.

3.4 Exemption to the Provision of Information

3.4.1 Personal Data processed for any of the following purposes:

i) the prevention or detection of crime; or

ii) the apprehension or prosecution of offenders, is exempt from the subject access provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

3.4.2 Each and every application will be assessed on its own merits and general blanket exemptions will not be applied.

3.5 Requests to Exercise Other Rights

3.5.1 Any request to exercise rights under Sections 10, 11 and 12 of the Data Protection Act 1998 will be directed in the first instance to the System Manager. The provisions of Sections 10, 11 and 12 of the Data Protection Act 1998 shall be followed in respect of every request.

3.6 Criminal Procedures and Investigations Act 1996

3.6.1 The Criminal Procedures and Investigations Act 1996 introduced a statutory framework for the disclosure to defendants of material, which the prosecution would not intend to use in the presentation of its case (known as unused material). Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the Data Controller by Section 7 of the Data Protection Act 1998 (known as subject access).

4 Accountability and Public Information

4.1 The Public

4.1.1 Cameras will not be used to look into private residential property.

4.1.2 A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the System Manager or completing the complaints form on Colehill Parish Council's website. All complaints shall be dealt with in accordance with the Owner's complaints procedure. Any performance issues identified will be considered under the Owner's disciplinary procedure to which all employees of the Owner and the Contractor are subject.

4.1.3 Where it is proved that an individual has suffered damage or distress by reason of any contravention of this Code that individual may be entitled to compensation.

4.2 System Manager

4.2.1 The System Manager shall have day-to-day responsibility for the System as a whole and is responsible for the effective control and administration of CCTV images.

4.2.2 The System Manager shall have unrestricted access to the footage and will maintain a log book(s) of incidents; to include incidents reported to the council and subsequently viewed, images released and to whom, complaints, maintenance, inspection and technical issues.

4.2.3 The System Manager shall ensure that every complaint is acknowledged in writing within five working days, which will include advice to the complainant of the enquiry procedure to be undertaken.

4.4 Public Information

4.4.1 A copy of this Code shall be published on the Owner's web site and a copy will be made available to anyone on request. Additional hard copies will be available at the Council's office.

4.4.2 Signs shall be placed in the locality of the camera. The signs will indicate:

- the presence of CCTV monitoring and the reason for monitoring;
- the Owner of the System;
- the contact telephone number for the Owner of the System.

5 Assessment of the System and the Code

5.1 Evaluation

5.1.1 The System shall be checked quarterly. The System and the Code will be evaluated annually at a Council meeting to establish whether the purposes of the System are being complied with and whether objectives are being achieved.

5.1.2 The evaluation shall include:

- An assessment of the incidents monitored by the System.
- The operation of the Code
- Whether or not the purposes for which the System was established are still relevant
- Cost effectiveness.

5.2 Monitoring

5.2.1 The System Manager shall have day-to-day responsibility for the monitoring, operation and evaluation of the System and the implementation of the Code.

5.2.2 The System Manager shall be responsible for maintaining full management information as to the incidents dealt with for use in the management of the System and in future evaluations.

6 Human Resources

6.1 Those responsible for the operation of the system

6.1.1 Only the Contractor shall operate the System equipment.

6.1.2 All personnel involved in the management and operation of the System shall have access to a copy of the Code, which may be updated from time to time. Staff must be fully conversant with the contents of the document which must be complied with as far as is reasonably practicable at all times. Breaches of the Code may be considered as a disciplinary matter.

6.1.3 All personnel involved in the System shall receive training from time to time in respect of all legislation appropriate to their role.

6.2 Discipline

6.2.1 All personnel with any responsibility under the terms of the Code and who have any involvement with the System will be subject to the Owner's disciplinary procedures. Any breach of the Code or of any aspect of confidentiality may be dealt with in accordance with those disciplinary procedures.

6.2.2 The System Manager has primary responsibility under the terms of the Code for ensuring that there is no breach of security and that the Code is complied with. Non-compliance with the Code by any person may be considered a breach of discipline and dealt with accordingly, including, if appropriate, the instigation of criminal proceedings.

7 Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 The cameras, control equipment, recording and reviewing equipment shall at all times be operated only by persons who have been trained in their use and the legislative implications of their use.

7.1.2 All use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with the Code.

7.1.3 The System operators must be mindful of exercising prejudices that may lead to complaints of the System being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time.

7.2 Control and Monitoring

7.2.1 Control and monitoring facilities will be provided to the System Manager at 15 Greenclose Lane, Wimborne via the Contractor downloading the footage.

7.4 Maintenance of the System

7.4.1 To ensure compliance with the Information Commissioner's Code of Practice and that images recorded continue to be of appropriate evidential quality, the System shall be maintained under a maintenance agreement.

7.4.2 The maintenance agreement will make provision for regular / periodic service checks on the equipment which will include cleaning of all weather domes or housings, checks on the functioning of the equipment and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.4.3 The maintenance agreement will also include regular periodic overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

7.4.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

7.4.5 It is the responsibility of the System Manager to ensure that appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance contractor.

8 Management of Recorded Material

8.1 Guiding Principles

8.1.1 For the purposes of the Code 'recorded material' means any material recorded by, or as the result of the use of, technical equipment which forms part of the System, and specifically includes images recorded digitally, or by way of video copying, including video prints.

8.1.2 Every digital recording obtained by using the System has the potential of containing material that may be required to be admitted in evidence at some point during its life span.

8.1.3 Members of the Public must have total confidence that information recorded about their everyday activities by virtue of the System will be treated with due regard to their individual right to respect for their private and family life.

8.1.4 It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy, video tape, CD or any form of electronic processing and storage) of the images obtained from the System, they are treated strictly in accordance with this Code and the provisions of the Data Protection Act from the moment they are received until final destruction.

8.1.5 Access to and the use of recorded material will be strictly for those purposes defined in the Code.

8.1.6 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

8.2 Release of Data to a Third Party

8.2.1 Every request for the release of Personal Data generated by the System will be channelled through the System Manager.The System Manager will ensure that the Good Practice Principles contained within Appendix C to the Code are followed at all times. Requests for access will be dealt with in accordance with ICO guidelines.

Information for individuals about how to make a request for access to their Personal Data is available on the Council's website.

Applicants will not be permitted to view recorded information, but may be offered the opportunity to view the images recorded of them in suitable Council accommodation made available to facilitate this where this is practicable and possible. 'Suitable' means private and not overlooked.

8.2.2 In complying with the Good Practice Principles for the release of Personal Data to third parties it is intended, as far as reasonably practicable, to safeguard the individual's right to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in the Code.
- Access to recorded material will only take place in accordance with the standards outlined in Appendix C to the Code.
- The release or disclosure of Personal Data for commercial or entertainment purposes is specifically prohibited.

8.2.3 Members of the Police or other agency having statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, release details of recorded information to the media where this is reasonably required to assist in the identification of alleged offenders or potential witnesses.

8.2.4 Full details of any recorded information originating from the System in whatever format for release to the media by the Police must be recorded and permission must be obtained from the System Manager prior to the release of any such material.

8.3 Retention of footage

8.3.1 The System is set to motion record and there is approximately 21 days of recording before it is overwritten.

8.3.2 Only the Owner's discs will be used. The Owner will not retain any copies. The Police or designated deputy may seize the 'Master disc'. Any further copies will be made by the police. Once the Master discs have been seized by the investigation officer that officer assumes ownership of the data (becomes the Data Controller) and is responsible for its security, evidential continuity and eventual destruction when it is no longer required. The Police become the Data Controller when any other data is transferred to their possession and control, for example video print or transfer of video footage into the 'police evidence locker'.

8.4 Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period in real-time.

Appendix A
Key Personnel and Responsibilities

1. System Owner:

Colehill Parish Council

Tel. 01202 900821

Responsibilities:

Colehill Parish Council is the Owner of the System.

The Owners will nominate a dedicated System Manager.

2. System Manager

The Clerk to the Council is the System Manager on behalf of the Owner. The System Manager will have delegated authority for data control on behalf of the Data Controller. This role includes responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the System in accordance with contractual arrangements, which the owner may from time to time enter in to.

ii) Ensure the interests of the Council are upheld in accordance with the terms of the Code.

iv) Authorise proposed alterations and additions to the System.

v) Maintain day to day management of the System.

vi) Accept overall responsibility for the System and for ensuring that the Code is complied with.

System Manager
Tracey Paine
15 Greenclose Lane
Wimborne BH21 2AL **Tel: (01202) 900821**

The Council's CCTV System Manager

The Council's CCTV Manager is responsible for the integrity, security, procedural efficiency and methods of operation of the System, including the gathering, retention and release of CCTV data.

This will include:
- management and training of any other Council officers authorised to assist in the operation of the System;
- the disclosure of information to the Police
- release of information to other third-parties who have a legal right to such information:
- maintenance of the quality of the recording and monitoring equipment.

The Council's System Manager will work in partnership with the Police with regard to the disclosure of information to the police for the purposes defined in the ISA. The Council's System Manager will consult with the Police in respect of any procedural or operational matters connected with the viewing or release of information to the Police.

Appendix B Data Protection Act 1998

Copies of the Act and the Information Commissioners Code of Practice can be downloaded from the website:

www.ico.gov.uk

Appendix C Good Practice for the Release of Data to Third Parties

1. Introduction

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

Colehill Parish Council is committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of information (data) which the system gathers.

After considerable research and consultation, the Owners have adopted the Good Practice Principles developed by The CCTV User Group.

2. General Policy

The Council is the body that determines the purpose for which and the manner in which any Personal Data are, or are to be processed.

All requests for the release of data shall be processed and channelled through the System Manager.

3. Primary Request to View Data

a) Primary requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:

   i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.)

   ii) Providing evidence in civil proceedings or tribunals

   iii) The prevention of crime

   iv) The investigation and detection of crime (may include identification of offenders).

   v) Identification of witnesses

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

   i) Police *(see note 1)*

   ii) Statutory authorities with powers to prosecute (e.g. Custom & Excise, Trading Standards, etc.)

   iii) Solicitors *(see note 2)*

iv) Plaintiffs in civil proceedings *(see note 3)*

v) Accused persons or defendants in criminal proceedings *(see note 3)*

vi) Other agencies, according to purpose and legal status *(see note 4)*

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

i) Not unduly obstruct a third party investigation to verify the existence of relevant data.

ii) Ensure the retention of data which may be relevant to the request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

d) In circumstances outlined in note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative shall:

i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.

ii) Treat all such enquiries with strict confidentiality.

Notes:

1) The release of data to the police is not to be restricted to the civil police but could include (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (Special arrangements may be put in place in response to local requirements)

2) Aside from criminal investigation, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

4) The data controller shall decide which (if any) 'other agencies' might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.

5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest hour).

4. Secondary Request to View Data

a) A 'secondary' request for access to data may be defined as any request being made

which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:

i) The request does not contravene and that compliance with the request would not breach current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000, section 163 Criminal Justice and Public Order Act 1994, etc.);

ii) Any legislative requirements have been complied with (e.g. the requirements of the Data Protection Act 1998, Freedom of Information Act 2000);

iii) Due regard has been taken of any known case law (current or past) which may be relevant (e.g. R v Brentwood BC ex p. Peck) and

iv) The request would pass a test of 'disclosure in the public interest' (see note 1).

b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in to place before releasing the material:

i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV Code of Practice.

ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV Code of Practice.

Notes:

1) 'Disclosure in the public interest' could include the disclosure of Personal Data that:

i) provides specific information which would be of value or of interest to the public well being

ii) identifies a public health or safety issue

iii) leads to the prevention of crime

2) The disclosure of Personal Data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request (see 3 above).

5. Individual Subject Access under Data Protection Legislation

a) Under the terms of the Data Protection legislation individual access to Personal Data, of which that individual is the data subject, must be permitted providing:

i) The request is made in writing

ii) A specified fee is paid for each search

iii) A data controller is supplied with sufficient information to satisfy him/herself as to the identity of the person making the request.

iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks (it is recognised that a person making a request may not know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement)

v) The person making the request is only shown information relevant to that particular search and which contains Personal Data of him/herself only, unless all other individuals who may be identified from the same information have consented to the disclosure.

b) In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied (all other Personal Data which may facilitate the identification of any other person should be concealed or erased).

c) The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merits.

d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

i) Not currently and as far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation.

ii) Not currently and as far as can be reasonably ascertained, not likely to become relevant to civil proceedings

iii) Not the subject of a complaint or dispute which has not been actioned

iv) The original data and that an audit trail has been maintained

v) Not removed or copied without proper authority

vi) For individual disclosure only (i.e. to be disclosed to a named subject)

6. Process of Disclosure

a) Verify the accuracy of the request.

b) Replay the data to the requester only (or responsible person acting on their behalf).

c) The viewing should take place in a separate room and not in the control room or monitoring area. Only data relevant to the request to be shown.

d) It must not be possible to identify any other individual from the information being shown (any such information will be blanked out, either by means of electronic screening or manual editing on the monitor screen.

e) If a copy of the material is requested and there is no on-site means of editing out other Personal Data, then the material shall be sent to an editing house for processing prior to being sent to the requester.

Note: *The Information Commissioners Code of Practice for CCTV makes specific*

requirements for the precautions to be taken when images are sent to an editing house for processing.

7. Media Disclosure

a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:

   i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.

   ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.

   iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System Code of Practice).

   iv) The release form shall be considered a contract and signed by both parties (see note 1)

Note:

In the well publicised case of R v Brentwood Borough Council, ex parte Geoffrey

Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted lawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid future accidental broadcasts. Attention is drawn to the requirements of the Information Commissioners in this respect, detailed in his Code of Practice summarised above.

8. Principles

In adopting these principles for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the system.

b) Access to recorded material shall only take place in accordance with this standard and the Code of Practice.

c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix D

Subject Access Request Form
COLEHILL PARISH COUNCIL CCTV SURVEILLANCE SYSTEM
Data Protection Act, 1998

Can be obtained from:

CCTV System Manager
Colehill Parish Council
15 Greenclose Lane
Wimborne
Dorset BH21 2AL

Telephone: 01202 900821

APPENDIX E

How to Apply For Access To Information Held On Council CCTV Systems

These notes explain how you can find out what information, if any, is held about you on Council CCTV Systems.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. Colehill Parish Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

The Council's Rights

Colehill Parish Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee of £75 is payable for each access request, which must be in pounds sterling. Cheques, postal orders, etc. should be made payable to **'Colehill Parish Council"**.

THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)

Section 1 Asks you to give information about yourself that will help the Council to confirm your identity. The Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2	Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full-face photograph of you.
Section 3	Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.
Section 4	**You must sign the declaration**

When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to:

THE SYSTEM MANAGER, COLEHILL PARISH COUNCIL,

15 Greenclose Lane, Wimborne BH21 2AL

COLEHILL PARISH COUNCIL CCTV SURVEILLANCE SYSTEMS

Data Protection Act 1998

SECTION 1 About Yourself

The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you.

PLEASE USE BLOCK LETTERS

Title *(tick box as appropriate)*	Mr		Mrs		Miss		Ms	
Other title *(e.g. Dr., Rev., etc.)*								
Surname/family name								
First names								
Maiden name/former names								
Sex *(tick box)*	Male				Female			
Height								
Date of Birth								
Place of Birth	Town							
	County							

Your Current Home Address *(to which we will reply)*	
	Post Code
A telephone number will be helpful in case you need to be contacted.	Tel. No.

If you have lived at the above address for less than 10 years, please give your previous addresses for the period:

Previous address(es)		
Dates of occupancy	From:	To:

SECTION 2 Proof of Identity

To help establish your identity your application must be accompanied by **TWO** official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.

Also a recent, full face photograph of yourself.

Failure to provide this proof of identity may delay your application.

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy YES /

(b) Only view the information YES /

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by Date

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

NOW – please complete Section 4 and then check the 'CHECK' box (on page 5) **before returning the form.**

SECTION 4 To Help us Find the Information

If the information you have requested refers to a specific offence or incident, please complete this Section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.

Were you: *(tick box below)*

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	

Other – please explain	

Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

Before returning this form	• Have you completed ALL Sections in this form?
Please check:	• Have you enclosed TWO identification documents?
	• Have you signed and dated the form?
	• Have you enclosed the £75.00 (seventy-five pound) fee?

Further Information:

These notes are only a guide. The law is set out in the Data Protection Act 1998, obtainable from The Stationery Office. Further information and advice may be obtained from:

The Office of the Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire, SK9 5AF.
Tel. (01625) 545745

Please note that this application for access to information must be made direct to **Colehill Parish Council** (address on Page 1) and **NOT** to the Information Commissioner.

OFFICIAL USE ONLY

Please complete ALL of this Section (refer to 'CHECK' box above).

Application checked and legible? ☐ **Date Application Received** ☐

Identification documents checked? ☐ Fee Paid ☐

Details of 2 Documents (see page 3) Method of Payment ☐

Receipt No. ☐

Documents Returned? ☐

Member of Staff completing this Section:

Name ☐ Location ☐

Signature ☐ Date ☐