Introduction

The purpose of this Policy is to regulate the review, management, operation, and use, of closed circuit television (CCTV) at Good Apple.

CCTV is in use to:

- increase personal safety of students, staff and visitors, and reduce the fear of crime
- monitor and minimise unauthorised and inappropriate access
- assist in managing the school
- protect the buildings and their assets
- support the Police in a bid to deter and detect crime
- assist in identifying, apprehending and prosecuting offenders
- protect members of the public and private property

This Code follows Data Protection Act guidelines and will be subject to review annually to include consultation as appropriate with interested parties.

1. The system

The CCTV system is owned by Good Apple and comprises 8 fixed and 4 moveable dome cameras located around the both sites, 7 internally and 2externally. All cameras are monitored from remote access and stored on DVR. The centralised system is only available to designated Management Team or their authorised nominee.

2. Statement of intent

2.1 The CCTV will be managed by the Directors and all the terms of the Data Protection Act 1998 and will endeavour to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

2.2 The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

2.3 Cameras will be used to monitor activities within the school for the purpose of securing the safety and well-being of the pupils, staff and visitors and to identify criminal activity actually occurring, anticipated, or perceived.

2.4 Staff have been instructed that static cameras are not to focus on private homes, gardens or other areas of private property.

2.5 Unless an immediate response to events is required, staff must not direct cameras off site at an individual, their property or a specific group of individuals, without an authorisation documented instruction from a member of the Senior Leadership Team or by police instruction endorsed by the Unit manager for Directed Surveillance, as set out in the Regulation of Investigatory Power Act 2000.

2.6 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. CD images/disks will only be released to the media for use in the investigation of a

specific crime and with the written authority of the police. CD images/disks will never be released to the media for purposes of entertainment.

2.7 Planning design and installation has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

2.8 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the school CCTV including entrance gates.

3. Operation of the system

3.1 The Scheme will be administered and managed by the Directors.

3.2 The day-to-day management will be the responsibility of both the unit manager an the directors.

3.3 The CCTV information will only be accessed by the director and / or police where necessary.

3.4 The CCTV system will be operated 24 hours each day, every day of the year.

4. System Equipment & Control

4.1 The Site Manager or his nominee will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

4.2 Access to the CCTV equipment will be strictly limited to the directors and unit manager.

4.3 Unless an immediate response to events is required, staff in the CCTV Control Room will not direct cameras at an individual or a specific group of individuals

4.4 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits to view information will not be permitted. 4.7 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

4.5 If out of hours emergency maintenance arises, the directors/ their representative must be satisfied of the identity and purpose of contractors before allowing entry.

4.6 A visitor's book will be maintained at school reception. Full details of visitors including time/date of entry and exit will be recorded.

5. Liaison

Liaison meetings may be held with all bodies involved in the support of the system eg police.

6. Monitoring procedures

6.1 Camera surveillance will be maintained at all times.

6.2 A monitor is installed in the office to which pictures will be continuously recorded.

6.3 Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with school policies and procedures and must be authorised by the Directors.

7. Image storage procedures

7.1 The images are stored on the CCTV Hard Drive in the Site Team office for a period of 10 days and are over written as the disk becomes full. If images are required for evidential purposes, the following procedures for their access, use and retention will be strictly adhered to:

7.1.1 The images required will be transferred to a disk which will be placed in a sealed envelope, witnessed, signed by the manager or assistant, dated and stored in a separate and secure safe, in the main Office, until collected.

7.1.2 Each disk will be identified by a unique reference number.

7.1.3 The disk used will be new or cleaned of any previous recording.

7.1.4 If the disk is archived at a later date, the reference number will be noted.

7.1.5 All disks made will be recorded in the CCTV Log.

7.2 Disks may be viewed by the Police for the prevention and detection of crime, authorised officers of the Local Authority for supervisory purposes, authorised demonstration and training.

7.3 A record will be maintained in the CCTV Log of the release of disks to the Police or other authorised applicants.

7.4 Viewing of disks by the Police will be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

7.5 Should a disk be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (i) of this Code. Disks will only be released to the Police on the clear understanding that the disk remains the property of the school, and both the disk and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon. On occasions when a Court requires the release of a disk copied from the CCTV system this will be produced and kept secure and made available as required.

7.6 The Police may require the school to retain the stored disks for possible use as evidence in the future. Such disks will be properly indexed and properly and securely stored in the Main Office until they are needed by the Police.

7.7 Applications received from outside bodies to view or release disks will be referred to the unit manager / dircetors. Requests from eg solicitors will normally be met where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

8. Access by or on behalf of the Data Subject

8.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate, and their parents, guardians or authorised carers) with a right to data held about themselves, including those obtained by CCTV.

8.2 A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

8.3 Requests for Data Subject Access should be made to the unit manager / dircetor and still images will be provided as per 8.1.(i) with the images of other pupils and adults obscured to prevent identification and inappropriate disclosure of their personal information.

9. Breaches of the code (including breaches of security)

9.1 Any breach of the Code of Practice by school staff will be investigated by the unit manager / directors or her nominee, and could lead to disciplinary action including dismissal.

9.2 Any serious breach of the Code of Practice will be immediately investigated and where appropriate an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, will be carried out by the Data Manager.

11. Data Retention

Recordings are made 24×7 and captured on the Site Office CCTV hard drive where they are retained for 10 days before being overwritten.

12. Public information

Copies of this Code of Practice will be available to the public via the school website or from the unit manager.

13. Complaints

13.1 Any complaints about the school's CCTV system should be addressed to the Directors..

13.2 Complaints will be investigated in accordance with Section 9 of this Code.

14. Summary of Key Points

14.1 The CCTV system is owned and operated by Good Apple.

14.2 This Code of Practice will be reviewed every year.

14.3 The unit or the Office will not be staffed out of school hours.

14.4 The Hard Drive may only be viewed by authorised Directors, Unit manager, or their nominee, and the Police.

14.5 The Office is not open to visitors except by prior arrangement and with approval.

14.6 Liaison meetings may be held with the Police and other bodies.

14.7 Moving images required as evidence will be properly recorded on disk from the Hard Drives, witnessed and packaged before copies are released to the police.

14.8 Stills images made available to individuals in response to individual requests will have other individual's images obscured to protect individual privacy.

14.9 Disks will not be made available to the media for commercial or entertainment.

14.10 Disks will be disposed of securely using the schools confidential waste arrangements which results in the disks being melted.

14.11 Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with academy policies and procedures and be authorised by the Directors. The Data Protection Co-ordinator for Schools, Education Department, provides additional information if required.

14.12 Breaches of the code and remedies will be reported to the Directors and o the unit manager.

14.13 Any breaches of this code will be investigated by the Directors. An independent investigation will be carried out for serious breaches.

Appendix 1B: CCTV Declaration Notices – Locations

- Main entrance.