

WORLE COMMUNITY SCHOOL

POLICY:

CCTV POLICY

Review date: 04/04/2011

1.0 INTRODUCTION

- 1.1 Closed Circuit Television (CCTV) has become a common feature of our daily lives. It necessarily involves intrusion into our lives but continues to enjoy public support when used responsibly and with effective safeguards in place.
- 1.2 The purpose of this policy is to regulate the management, operation and use of the CCTV system at Worle Community School hereafter referred to as 'the school'. The system comprises a number of internal and external cameras located around the school site; for security reasons the number and location of these cameras has not been specified in this document. All cameras are either wall or ceiling mounted and linked to a number of hard disk recorders. The CCTV system is owned by the school with the Business Manager the nominated person who oversees the system and the procedures.

2.0 OBJECTIVES OF THE CCTV SCHEME

- 2.1 The objectives of the scheme are;
- To protect the school buildings, grounds and their assets;
 - To increase personal safety and reduce the fear of crime;
 - To support the Police in a bid to deter and detect crime;
 - To assist in identifying, apprehending and prosecuting offenders;
 - To assist in managing the school.

3.0 STATEMENT OF INTENT

- 3.1 The schools CCTV system being wall/ceiling mounted and not able to follow a particular person or event, does not require to be registered with the Information Commissioner. However, the schools intent is that it will comply with the overall requirements and intent of the Data Protection Act 1988 and the Commissioners Code of Practice.
- 3.2 The school will treat the system and all information, documents and recordings obtained as data which are protected by the act.
- 3.3 Cameras will be used to monitor activities within the school car park and along footpaths around the school. Cameras located in some classrooms are activated only after the school day has terminated and will be automatically turned off before commencement of school. The camera within the Exclusion Room will be active during the school day.

- 3.4 Cameras are positioned around the school so as not to overlook private homes, gardens and other areas of private property.
- 3.5 Material or knowledge secured as a result of CCTV will not be used for any commercial purpose. DVDs will only be released to external agents, such as the Police, if required for use in the investigation of a specific crime or incident. DVDs will never be released to the media for the purpose of entertainment.
- 3.6 The location of the School's CCTV has been carefully planned to give maximum effectiveness but due to the large school site it is not possible to guarantee that the system will cover all areas of the school and detect all incidents of crime.
- 3.7 Warning signs as required by the Information Commissioners Code of Practice confirming that CCTV is in operation at the school have been placed at access routes in to the school and also around the school.
- 3.8 There is no means of audio recording within the system.

4.0 OPERATION OF THE SYSTEM

- 4.1 The scheme will be administered and managed by the Business Manager, in accordance with the principles and objectives expressed in the code.
- 4.2 The day-to-day management will be the responsibility of the Business Manager, Network Manager, Site Manager and the Site Team.
- 4.3 The CCTV system outside of classrooms may be operated at any time, day or night throughout the year.

5.0 EQUIPMENT

- 5.1 The Site Team will check and confirm the efficiency of the system weekly and in particular that the equipment is properly recording and that cameras are functional.
- 5.2 Access to the CCTV will be strictly limited to the Site Team or appointed contractor. Further access may be granted by the Business Manager.
- 5.3 Cameras may not be relocated or re-positioned without the agreement of the Business Manager.
- 5.4 If out of hours emergency maintenance arises, the Site Team member must be satisfied of the identity and purpose of the contractor before allowing access to the site and system.
- 5.5 When required, the Network Manager will be requested to produce a DVD of an incident or occurrence. The Network Manager must maintain a log of all such requests and details of who requested the DVD, what the DVD contained and who was given the DVD.
- 5.6 The internal data recorders will automatically record images from the cameras and store the data on the hard drives for a period of 30 days after which the recordings

are automatically deleted. It is therefore essential that if data is required for long-term storage that the Network Manager be informed such that data can be transferred to a DVD.

6.0 MONITORING PROCEDURES

6.1 Camera surveillance may be conducted at any time.

6.2 The following personnel have the ability to monitor CCTV data:

Site Manager
Site Team
Network Manager
Receptionist

7.0 DVD PROCEDURES

7.1 In order to maintain and preserve the integrity of the discs used to record events from the system and the facility to use them in any future proceedings, the following procedures for the use and retention must be strictly adhered to:

a. Only previously unused DVDs should be used to record data.

b. Each DVD must be identified by a unique individual number.

c. A register is to be maintained which contains the individual DVD number, the date/time of images stored and the camera reference. The Network Manager shall maintain the register.

d. A DVD required for evidential purposes must be sealed, witnessed, signed by the Network Manager dated and stored in a secure location before being handed to the Police. The transfer of a DVD to the Police must be signed for.

e. If a DVD is held at school, the storage location of the DVD are to be recorded on the register.

7.2 Data contained on the systems hard drive or disks may be viewed by the Police for the prevention and detection of crime. In general, pupils and the public are not permitted to view data stored on the systems hard drive or discs without the authorisation of the Business Manager.

7.3 A record is to be maintained by the Network Manager of all disks released to the Police or other authorised applicants. A register is to be maintained for this purpose.

7.4 Viewing of discs or the hard drive by the Police or other authorised individuals must be recorded in the register. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1988.

7.5 Applications received from outside bodies (eg solicitors) to view or release discs will be referred to the Business Manager. Discs will be released where satisfactory documentary evidence is produced showing that they are required for legal

proceedings, a subject access request or in the response to a court order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials, postage and the administrative time taken to produce such disc in other cases.

- 7.6 Images will be retained on the hard drive for a period of 30 days and then they will automatically be overwritten. If data is required beyond this period a copy will be taken and stored securely inline with the procedures above.
- 7.7 A DVD held on school property will be destroyed at an appropriate time. This destruction will be documented by the Network Manager and kept with the register.

8.0 BREACHES OF THE CODE

- 8.1 Any breach of the Code of Practice by school staff will be initially investigated by the Head Teacher who may consider it appropriate to take disciplinary action against an individual.
- 8.2 Any serious breach of the Code of Practice will be referred for investigation by the school Governors; a minimum of 3 Governors will be convened so that recommendations on how to remedy the breach may be made. Disciplinary action may be taken against an individual found to have acted in contravention of the Code of Practice.

9.0 ASSESSMENT OF THE SCHEME AND CODE OF PRACTICE

- 9.1 Performance monitoring, including random operating checks, may be carried out by the Site Manager and Business Manager at any time.

10.0 COMPLAINTS

- 10.1 Any complaint about the school's CCTV system should be addressed to the Head Teacher in writing. Complaints will be investigated by an appropriate member of staff depending on the nature of the complaint.

11.0 ACCESS BY THE DATA SUBJECT

- 11.1 The Data Protection Act provides Data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV. However, where images include individuals, particularly children, other than the subject individual, permission by those individuals will be required before any data is issued. Therefore the release of data to subject can not be guaranteed.
- 11.2 Requests for Data Subject Access should be made in writing to the Business Manager, specifying the date, time and location of the image required.