A Specialist School for ICT

Ashfield Girls' High School

CCTV Policy

Ashfield Girls' High School
CCTV Code of Practice

1. Introduction

1.1. **The Strategic Partnering Agreement** (Clause 82) hereafter referred to as 'SPA' states that the contractor, namely Amey Built Environment hereafter referred to as 'AMEY BE' shall at all times comply with the Data Protection Act 1998 hereafter referred to as 'DPA' and shall not disclose personal data to any third parties other than its employees and sub-contractors and shall bring into effect all technical and organisational measures to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction or damage to data.

The AMEY PLC Code of Practice Document Governing the Operation of the CCTV System has been issued with due regard to the 'DPA' and the associated British Standard 7958: 1991 "Closed Circuit Television (CCTV). The Code of Practice is a strategic document with governs the management and operation of the CCTV System, CCTV Recording and CCTV Processing Facilities at **Ashfield Girls' High School** hereafter referred to as AGHS

1.2. The purpose of this Policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) system at **AGHS**

1.3. The Data Controller hereafter referred to as 'DC' is responsible for ensuring that their processing complies with the Data Protection Act 1998 (DPA).

1.4. The 'DC' for **core times** is **AGHS** as defined within the Strategic Partnering Agreement (SPA)

1.5. The 'DC' for **non core times** is 'Amey BE' as defined within the Strategic Partnering Agreement (SPA)

1.6. The system comprises a number of fixed dome and PTZ [pan tilt zoom] cameras located in and around the school site. External cameras are monitored from the 'Amey BE' offices and internal cameras are monitored from the main school office images are only available to selected senior staff.

1.7. This code follows 'DPA' guidelines.

1.8. The code of practice will be subject to review regularly and include consultation as appropriate with interested parties.

1.9. The CCTV system is owned and operated by 'Amey BE' as the Data Processor.

2. Objectives of the CCTV system

2.1. To protect pupils, staff and visitors

2.2. To increase personal safety and reduce the fear of crime

2.3. To protect the school buildings and assets

2.4. Without prejudice, to protect the personal property of pupils, staff and visitors.

2.5. To support the police in preventing and detecting crime

2.6. To assist in identifying, apprehending and prosecuting offenders

2.7. To assist in managing the school

3. Statement of intent

3.1. The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

3.2. The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

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

3.3.1. The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.

3.4. Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose.

3.4.1. Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.

3.4.2. Images will never be released to the media for the purposes of entertainment.

3.5. The planning and design has endeavoured to ensure that the system 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.

3.6. Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by the school CCTV system.

4. System Management (Ref: Appendix A)

4.1 The system will be administered and managed by the 'DC' who will act as the 'DC' in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of both the senior management team and the 'Data Processor' namely 'Amey BE' who will act as the system manager

4.3 The Data Processor (DP) is defined in relation to personal data as any person (other than an employee of the Data Controller) who processes the data on behalf of the data controller

4.4 The system and the data collected will only be available to the Data Controller, the senior management team and the System Manager.

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

4.6 The System Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

4.7 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

4.8 The System Manager must satisfy him/her self of the identity of any person wishing to view images and the legitimacy of the request. Where any doubt exists access will be refused.

4.9 Details of all requests will be recorded in the system log book including time/date of access and details of images viewed.

4.10 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

4.11 If out of hours emergency maintenance arises, the System Manager must be satisfied of the identity and purpose of contractors before allowing access to the system.

5. Liaison

5.1 Liaison meetings may be held with all bodies involved in the support of the system

6. Video tape viewing and download media procedures

6.1 In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any tape or download media used to record events must be prepared in accordance with the following procedures:

6.1.1 Each tape or download media must be identified by a unique mark.

6.1.2 Before use, each tape or download media must be cleaned of any previous recording.

6.1.3 The System Manager will register the date and time of tape or download media insertion, including its reference.

6.1.4 A tape or download media required for evidential purposes must be sealed, witnessed, signed by the System Manager, dated and stored in a secure store. If a tape or download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the System Manager, dated and returned to the secure store.

6.1.5 If tapes or download media is archived the reference must be noted.

6.2 Images may be viewed by the police for the prevention and detection of crime and by authorised Belfast Education and Library Board Officers for supervisory purposes, authorised demonstration and training.

6.3 A record will be maintained, by the system manager, of the release of tapes or download media to the police or other authorised applicants. A register will be available for this purpose.

6.4 Viewing of images by the police must be recorded in writing and in the log book.

6.5 Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the tape or download media (and any images contained thereon) remains the property of the school, and both the tape or download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the tape or downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of an original tape or downloaded media this will be produced from the secure store, complete in its sealed bag.

6.6 The police may require the school to retain the stored tapes or downloaded media for possible use as evidence in the future. Such tapes or downloaded media will be properly indexed, by the system manager, and properly and securely stored until they are needed by the police.

6.7 Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Principal. In these circumstances tapes or downloaded media will normally be released 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. The following fees can be charged in such circumstances: -

6.7.1 £10 for subject access requests

6.7.2 A sum not exceeding the cost of materials in other cases.

7 Breaches of the code (including breaches of security)

7.1 Any breach of the code of practice by school staff will be initially investigated by the Data Controller (Amey BE/**AGHS** in order for him/her to take the appropriate action.

7.2 Any serious breach of the code of practice will be the subject of an immediate independent investigation. The investigation will also make recommendations on how to remedy the breach. Any further action or recommendations will be referred to the relevant statutory body.

8 Assessment of the system and code of practice

8.1 Performance monitoring, including random operating checks, may be carried out by the Data Controller.

9 Complaints

9.1 Any complaints about **AGHS'** CCTV system should be addressed to the Data Controller.

10 Access by the Data Subject

10.1 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.

10.2 Requests for Data Subject Access should be made in writing, outlining the reason for the request, to the Data Controller.

11 Public information

11.1 Copies of this code of practice will be available to the public on request from the school office and the Principal.

12 Summary of key points

12.1 This code of practice will be reviewed regularly

12.2 The **[external]** CCTV system is owned and operated by Amey BE. **[The internal CCTV system is owned by the school and operated by Amey BE]**

12.3 The CCTV system and images are not available to visitors except by prior arrangement and good reason

12.4 Recording tapes or downloaded media will be used properly indexed, stored and destroyed after appropriate use.

12.5 Images may only be viewed by authorised personnel as described in this document

12.6 Tapes or downloaded media required as evidence will be properly recorded witnessed and packaged before copies are released to the police

12.7 Tapes or downloaded media will not be made available to the media for commercial or entertainment purposes.

12.8 Tapes or downloaded media will be disposed of securely by incineration

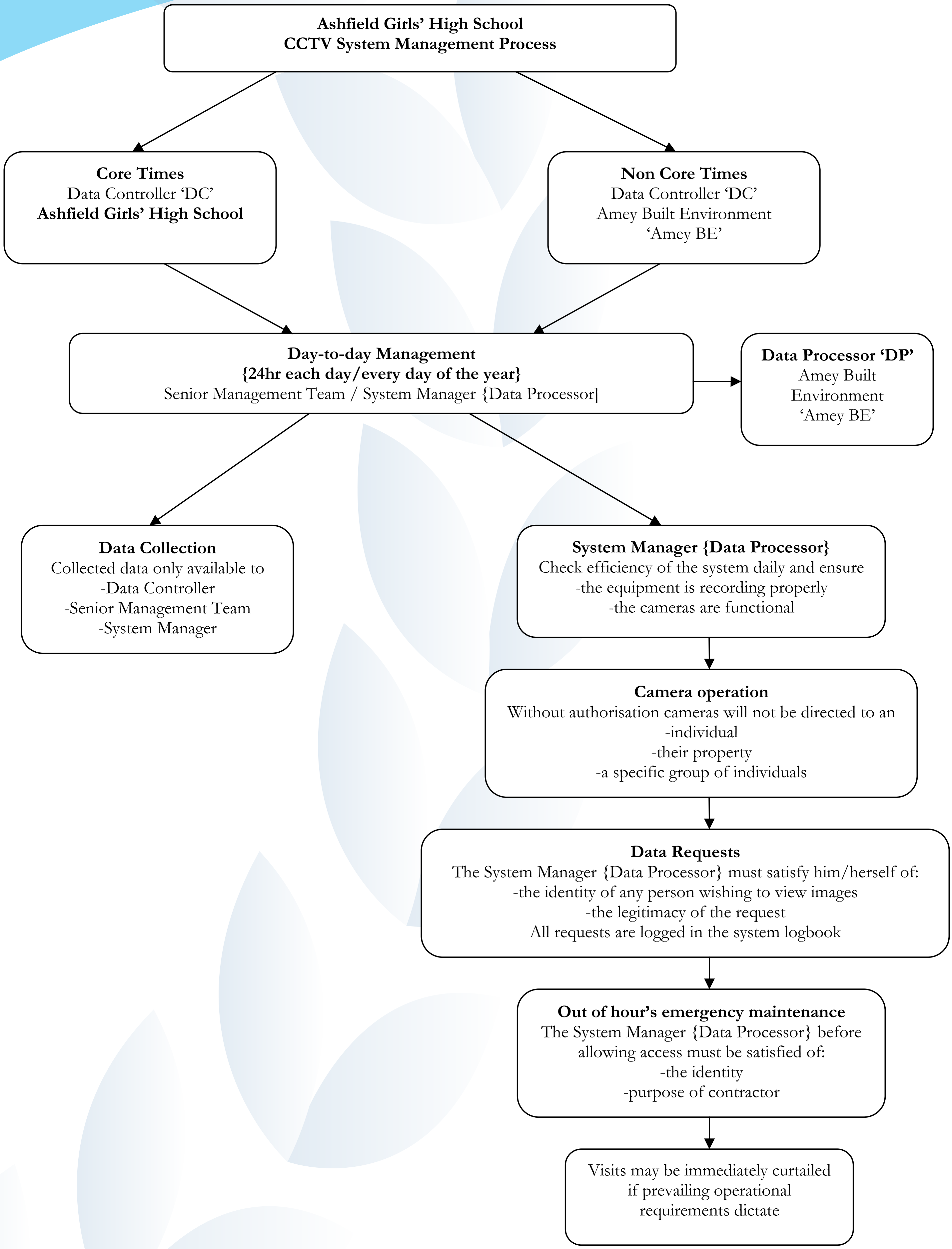
12.9 Any covert surveillance being considered or planned as part of an operation should be discussed with the Belfast Education and Library Board Security Advisor.

12.10 Any breaches of this code will be investigated by the Data Controller. An independent investigation will be carried out for serious breaches.

12.11 Breaches of the code and remedies will be reported to the Data Controller.

13. This document was produced January 2011

Appendix A



Ashfield Girls' High School
CCTV System Management Process

Core Times
Data Controller 'DC'
Ashfield Girls' High School

Non Core Times
Data Controller 'DC'
Amey Built Environment
'Amey BE'

Day-to-day Management
{24hr each day/every day of the year}
Senior Management Team / System Manager {Data Processor]

Data Processor 'DP'
Amey Built
Environment
'Amey BE'

Data Collection
Collected data only available to
-Data Controller
-Senior Management Team
-System Manager

System Manager {Data Processor}
Check efficiency of the system daily and ensure
-the equipment is recording properly
-the cameras are functional

Camera operation
Without authorisation cameras will not be directed to an
-individual
-their property
-a specific group of individuals

Data Requests
The System Manager {Data Processor} must satisfy him/herself of:
-the identity of any person wishing to view images
-the legitimacy of the request
All requests are logged in the system logbook

Out of hour's emergency maintenance
The System Manager {Data Processor} before
allowing access must be satisfied of:
-the identity
-purpose of contractor

Visits may be immediately curtailed
if prevailing operational
requirements dictate

Last Updated: November 2013

INVESTORS IN PEOPLE | Bronze

A Specialist School for ICT

ICT MARK ACCREDITED

NEXT GENERATION LEARNING

Eco-Schools

iNet

International Networking for Educational Transformation™

C2K

DELIVERING TECHNOLOGY FOR LEARNING

Microsoft Partners in Learning

Worldwide Innovative Education Forum

3rd

SSAT

inquire
Inspire
Innovate
Impact

PTA-UK gold★awards 2012

Principal: Mrs A Mungavin BA DipEd PQH (NI)
Holywood Road • Belfast • BT4 2LY • Tel: 028 90471744 • Fax: 028 90672416
E-Mail: info@ashgirls.belfast.ni.sch.uk • Internet: www.ashfieldgirls.org