BASTION
COMPLETE SECURITY Ltd.
0844 870 9859
CCTV | Access Control | Gate Automation
Door Entry | Public Address | Data
Fire Alarms | Audio Visual

www.bastioncompletesecurity.co.uk
No. 8 Clipper Park, Thurrock Park Way, Tilbury, Essex. RM18 7HG
Installation and maintenance of Electronic Security Systems office@bastioncompletesecurity.co.uk

COMPLIANCE

Compliance Documentation

For the

CCTV Security System

Installed at

Mark Hall Academy

First Avenue, Harlow Essex. CM17 9LT.

Prepared by

Greg Foster
Project Manager
1st June 2016

Checked and passed by

Graham R Gardener
Managing Director
1st June 2016

Annual Review for the Operation of a CCTV Surveillance System

Mark Hall Academy

First Avenue. Harlow, Essex. CM17 9LR

June 2016

This document has been prepared by Bastion Complete Security Ltd., based on information supplied to us by Mark Hall Academy and as such the information contained herein is to the best of our knowledge true and correct at the time of publication and that we have not knowingly misrepresented the information supplied to us.

Copyright Notice

Index

Section

Section 1
Details of the System Operator and Data Controller

The system operator is;

Mark Hall Academy

The data controller is;

The Academy Transformation Trust

The system is registered with the Information Commissioners Office, Data Protection Register and the details of the registration are;

Registration Number: Z3277414

Date Registered: 2nd August 2012 Registration Expires: 1st August 2016

Data Controller: The Academy Transformation Trust

Address: Room 501, 1 Victoria Square, Birmingham, B1 1BD

This data controller does not state that it is a public authority under the Freedom of Information Act 2000

Section 2
Executive Summary

Following the recommendations in the 2015 annual review for the operation of a CCTV surveillance system a system upgrade has been completed. As a result of this upgrade all the relevant compliance issues identified in last year's review have been addressed and it is on this basis that the current review has been prepared.

Founded in 1950, Mark Hall Academy is a coeducational secondary school located in Harlow which provides education to approximately 550 children between the ages of 11 – 16. The school has academy status and is sponsored by the Academy Transformation Trust.

This annual assessment has been prepared by Bastion Complete Security Ltd in consultation with Mark Hall Academy and forms part of the compliance documentation in support of the ownership and continued operation of an existing CCTV system. We have prepared this assessment in accordance with the principles set out in the Information Commissioner's Code of Practice and the Surveillance Commissioner's Code of Practice.

These codes of practice recommend that Privacy Impact Assessments should be carried out on a regular basis, at least annually, to ensure that existing CCTV systems comply with the relevant legislation in which context they are set and this is included in Section 6 of this document.

Please note that items printed in green are summaries of the code and principle referenced in the preparation of this report. All items printed in black refer to those which are relevant or specific to Mark Hall Academy.

Section 3
Policy Statement for the Operation of a CCTV Monitoring System

Mark Hall Academy is committed to ensuring the safety and wellbeing of all staff, students and visitors to the site.

In order to support this objective, we own and operate a CCTV monitoring system, which not only assists us in providing a safe and secure environment, but is also a valuable tool for deterring crime and protecting assets.

In accordance with our documented procedures for the operation of the CCTV System, Mark Hall Academy will ensure that this system is compliant with both the Information Commissioner's Code of Practice and the Surveillance Commissioner's Code of Practice. Compliance with these codes will help us to use surveillance cameras to collect personal data whilst staying within the law.

For the purposes of this document and to pre-empt future extensions by secondary legislation to the definition of a "relevant authority" as defined by the Protection of Freedoms Act 2012 Section 33 (5), we acknowledge the recommendation of the Surveillance Commissioner to follow the 2013 Surveillance Camera Code of Practice and the responsibilities placed upon us as an organization by the 2012 Act and the following primary legislation;

Data Protection Act 1998
Freedom of Information Act 2000
Human Rights Act 1998

It is within this legislative framework that we operate the CCTV surveillance system.

Section 4
Annual Assessment of Compliance with the Surveillance Camera Commissioner's Code of Practice

Principle 1

Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified and pressing need

1. *Have you translated principle 1 into clear objectives? If so what are they?*
2. *Do you regularly review the system and assess against the objectives?*
3. *Have you considered the requirement of the end user?*
4. *Is the system being used for any other purpose than those specified? If so please explain.*
5. *Have you identified any areas where further action is required to more fully conform to the requirements of Principle 1? Is there an Action Plan?*
6. *Assist in the provision of a safe and secure environment for the benefit of those who might visit, work or study on the site.*
7. *Reduce the fear of crime by reassuring staff, students and visitors.*
8. *Deter and detect crime, disorder, or anti-social behaviour.*
9. *To identify, apprehend and prosecute offenders in relation to crime, disorder, or anti-social behaviour.*
10. *Provide the police or law enforcement agencies and the (Insert Organisation Type e.g. School, Company) with evidence upon which to take criminal, civil or disciplinary action as appropriate.*

1.1 The purpose for the installation and continued operation of a camera surveillance system is to achieve the following objectives;

Enhance the personal safety and security of all persons using the site.
Reduce the fear of crime, or antisocial behaviour
The prevention, deterrence, detection and prosecution of crime, or antisocial behaviour
Support the disciplinary process in the event of crime or antisocial behaviour
The protection and security of valuable assets

1.2 The Review Process
This is the second annual review of the surveillance camera system. The surveillance camera system is subject to an annual review which takes place annually in June.

1.3 Requirements of the End User
Images captured and stored by the system must be of sufficient quality to ensure their value for evidential purposes. Last year it was identified that some aspects of the technical specification and performance of the system may not have reached these requirements and an order was placed with an installation contractor and a system upgrade and extension has recently been completed and as a result these issues have now been resolved.

1.4 System Use
The system is not used for any other purposes than those identified in 1.1 above

1.5 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 1

Principle 2

The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified

1. *Do you review your system annually?*
2. *Have you conducted a privacy impact assessment?*
3. *Do you publish your privacy impact assessment and annual review?*
4. *Have you identified any areas where further action is required to more fully conform to the requirements of Principle 2? Is there an action plan?*

2.1 The Annual Review Process

The surveillance camera system is subject to an annual review which takes place annually in June

2.2 Privacy Impact Assessments

The surveillance camera system is subject to an annual privacy impact assessment which takes place annually in June.

2.3 Publication Details

The governing body has approved the publication of this document on the school's website

2.4 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 2

Principle 3

There must be as much transparency in the use of the surveillance camera system as possible, including a published contact point for access to information or complaints.

1. *Does signage exist highlighting the use of surveillance cameras?*
2. *Does the signage highlight the point of contact?*
3. *Has there been proportionate consultation and engagement with the public and partners to establish that there is a legitimate aim and a pressing need for the surveillance camera system?*
4. *Is the surveillance system a proportional response?*
5. *Does your publication of information include the procedures and safeguards that are in place, impact assessments undertaken, performance statistics and any other management information?*
6. *Do you have a complaints procedure in place?*
   Do you make the public aware of how you escalate complaints?
   Is there a defined time scale for acknowledging and responding to complaints and is this conveyed to the complainant at the outset?
   Do you publish the number and nature of complaints received?
7. *Have you identified any areas where further action is required to more fully conform to the requirements of Principle 3? Is there an Action Plan?*

3.1 Signage and Warning Notices

The signage and warning notices that CCTV surveillance and recording is in operation formed part of the system upgrade program and is now deemed to be adequate to meet the requirements of the Code of Practice.

3.2 Points of Contact

The signage and warning notices which have been installed as part of the upgrade program highlight a point of contact where further information may be obtained about the operation of the CCTV system.

3.3 The Consultation Process

The following individuals or groups will be consulted annually to establish that there is a legitimate aim and pressing need for the continued operation of a CCTV surveillance system.

The Academy Transformation Trust
The Principal
The Operations Director
The Local Governing Body

3.4 Proportionality

Having conducted this review the individuals or groups identified above have agreed that the continued operation of a surveillance camera system is a proportionate response to achieve the objectives set out in Section 1.1 above.

3.5 Publication Details

This annual review forms part of the published information on the operation of the surveillance camera system and contains information related to procedures and safeguards which are in place, together with the annual compliance review for the purposes of the Information Commissioner's Code of Practice and the Surveillance Camera Commissioner's Code of Practice.

3.6 Complaints Procedure

The point of contact for processing any complaints that may arise in connection with the operation of the surveillance camera system will be the Operations Director. Complaints will be logged and will be acknowledged within 7 working days. Should further investigation be required the complainant will receive a response within 30 days from the date at which the complaint was first logged.

No complaints in respect of the operation of the CCTV system were received during the preceding year.

3.7 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 3

Principle 4

There must be clear responsibility and accountability for all surveillance camera activities including images and information collected, held and used.

1. *What arrangements are in place to provide clear responsibility and accountability?*
2. *Are all staff aware of their responsibilities?*
3. *Explain how you ensure these lines of responsibility are adhered to*
4. *If jointly owned, is it clear what each partner organization is responsible for and what the individual obligations are?*
5. *Have you identified areas where further action is required to more fully conform to the requirements of Principle 4?*

4.1 Responsibility and Accountability

The person responsible for the operation and management of the system is the Operations Director and is accountable to the Principal. The Site Manager and all staff authorized and involved with the operation of the system are accountable to the Operations Director. All staff authorized and involved with the operation of the surveillance camera system are trained in that operation. As part of the training process they are made aware of and issued with the relevant codes of practice.

4.2 Staff Awareness

All staff authorized and involved with the operation of the surveillance camera system are aware of their responsibilities and the person to whom they are accountable.

4.3 Joint Responsibility

The surveillance camera system is not jointly owned, therefore delineation of responsibilities to partner organizations is not applicable.

4.2 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 4

Principle 5

Clear rules, policies and procedures must be in place before the surveillance camera system is used and these must be communicated to all who need to comply with them.

1. *There are significant benefits in having clear policies and procedures for the operation of any surveillance. This can not only aid the effective management and use of the surveillance camera system, but also help to ensure that any legal obligations affecting the use of such a system is addressed*
2. *A surveillance camera system operator is encouraged to follow a quality management system as a major step forward in controlling and improving their key processes. Where this is done through certification against a quality management standard it can provide a robust operating environment with additional benefit of reassurance for the public that the system is operated responsibly and effectively and that the likelihood of any breach of individual privacy is greatly reduced.*
3. *It is good practice that the communication of rules, policies and procedures should be done as part of the induction and ongoing professional training and development of all system users. This should maximise the likelihood of compliance by ensuring system users are competent have relevant skills and training on the operational, technical and privacy considerations and fully understand the policies and procedures. It is a requirement of the 1998 Act that organisations ensure the reliability of staff having access to personal data, including images and information obtained by the surveillance camera system*
4. *Wherever there are occupational standards available which are relevant to the roles and responsibilities of their system users, a systems operator should consider the benefits and statutory requirements associated with such occupational standards.*
5. *The Surveillance Camera Commissioner will provide advice and guidance on relevant quality management and occupational competency standards.*
6. *Wherever a surveillance camera system covers public space a system operator should be aware of the statutory licensing requirements of the Private Security Industry Act 2001. Under these requirements the Security Industry Authority (SIA) is charged with licensing individuals working in specific sectors of the private security industry. A public space surveillance (CCTV) license is required when operatives are supplied under a contract for services. It is a criminal offence for staff to carry out licensable activities without an SIA license.*
7. *SIA licensing is dependent upon evidence that an individual is fit a proper to fulfil the role and evidence of their ability to fulfil a role effectively and safely with the right skills and knowledge. There are various relevant qualifications available and training to attain these is delivered by a range of accredited providers.*
8. *Even where there is no statutory licensing requirement, it is good practice for a system operator to ensure that all staff who either manage or use a surveillance camera system, or use or process the images and information obtained by virtue of such systems have the necessary skills and knowledge*

5.1 Policies, Procedures and Operating Instructions

Policies, procedures and operating instructions for the CCTV system are held by the Operations Director and the Site Manager.

5.2 Quality Management System

The organisation does not operate a quality management system and the operation of the CCTV system is not part of a QMS

5.3 Training & Development

All staff authorized and involved with the operation of the surveillance camera system are trained in that operation. As part of the training process they are made aware of and issued with the relevant codes of practice.

5.4 The Private Security Industry Act 2001

The camera surveillance system does not cover a public space and is therefore not subject to the above Act and an SIA licence is not required.

5.5 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 5

Principle 6

No more images and information should be stored than that which is strictly required for the stated purpose of the surveillance camera system and such images and information should be deleted once their purposes have been discharged.

1. *Images and information obtained from a surveillance camera system should not be kept for longer than is necessary to fulfil the purpose for which they were obtained in the first place. This period should be decided in advance and be the minimum period necessary. This is also a requirement of the 1998 Act and further guidance on this is contained in the ICO CCTV Code of Practice.*
2. *The retention period for different camera surveillance systems will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose. It is not, therefore possible to be prescriptive about minimum and maximum retention periods. Initial retention periods should be reviewed by a system operator and reset in the light of experience. A proportionate approach should always be used to inform retention periods and these should not be based on infrequent exceptional cases.*
3. *Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions a system operator may need to retain images for a longer period, for example when a law enforcement body is investigating a crime to give them an opportunity to view the images as part of an active investigation*.

6.1 Retention Period

Following completion of the system upgrade the retention period has been set to a maximum of 30 days which will ensure that operational requirements are met and preclude the possibility that personal data is not stored for longer than is necessary to meet those requirements. When the stored data has exceed 30 days it is securely destroyed by data overwrite

6.2 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 6

Principle 7

Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or law enforcement purposes

1. *The disclosure of images and other information obtained from a surveillance camera system must be controlled and consistent with the stated purpose for which the system was established. Disclosure of images or information may be appropriate where the 1998 Act makes exemptions which allow it, provided that the applicable requirements of the 1998 Act are met, or where permitted by other legislation such as the Counted Terrorism Act 2008. These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime and for national security purposes. Where a system operator declines a request for disclosure from a law enforcement agency there is provision under Section 9 of and Schedule 1 to the Police and Criminal Evidence Act 1984 to seek a production order from a magistrate.*

2. *There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. Such requests for images or information should be approached with care and in accordance with the 1998 Act, as a wide disclosure may be an unfair intrusion into the privacy of the individuals concerned.*

3. *A system operator should have clear policies and guidelines in place to deal with any requests that are received. In particular;*
   - *Arrangements should be made to restrict disclosure of images in a way consistent with the purpose for establishing the system.*
   - *Where images are disclosed, consideration should be given to whether the images of individuals need to be obscured to prevent unwarranted identification*
   - *Those that may handle requests for disclosure should have clear guidance on the circumstances under which disclosure is appropriate.*
   - *The method of disclosing images should be secure and ensure that they are only seen by the intended recipient.*
   - *Appropriate records should be maintained.*
4. *Judgements about disclosure should be made by the system operator. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once they have disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image. If the recipient is a relevant authority, then it is the recipient's responsibility to have regard to this code of practice and to comply with any other legal obligations such as the 1998 Data Protection Act and the Human Rights Act 1998 in relation to further disclosures.*
5. *Individuals can request images and information about themselves through a subject access request under the 1998 Act. Details on this and matters such as when to withhold images of third parties caught in images is included in the ICO CCTV Code of Practice*
6. *Request for information from public bodies may be made under the Freedom of Information Act 2000. Detailed guidance on these obligations is included in the ICO CCTV Code of Practice.*

7.1 Access to Images

Access to stored images is restricted to the following staff and is consistent with the stated objectives of operating the system

The Operations Director
The Site Manager
Member of the Site Team

7.2 Disclosure to Third Parties

Disclosure of stored images to third parties is strictly controlled and is consistent with the stated purpose for which the system is deployed.

Disclosure of stored images will be made to following third parties provided that they meet certain criteria consistent with the stated purpose for which the system is deployed.

The Police or any law enforcement agency to assist in the process of a criminal investigation or the prosecution of a crime.

The order of the Criminal or Civil Court

At the request of the Principal, or members of the Academic Leadership Team which comprises 8 senior staff in order to assist in the investigation of crime, vandalism or antisocial behaviour and in the subsequent disciplinary process where appropriate. Exceptionally, it may be necessary to allow a most relevant person to view an image for the purposes of identification

Under exceptional circumstances request for disclosure requests by other third parties will be considered. For example a request by a person whose property has been damaged may be appropriate. Such requests will be approached with great care and in accordance with the principles of the Data Protection Act 1998 and where granted will be as limited as possible to ensure that there is no unfair intrusion into the privacy of the individuals concerned.

Any third party disclosure will be subject to the following policy and guidelines for dealing with such disclosure requests

7.3 Disclosure Policy

Disclosures to third parties are made at the sole discretion of the Data Controller and any request for access may be denied unless there is an overriding legal obligation such as a court order

No disclosure will be made which is inconsistent with the specified purpose for which the operation of the system was established.

Consideration will always be given to whether images of individuals need to be obscured to prevent unwarranted identification which would not be consistent with the principles of the Data Protection Act 1998.

We recognise as the system operator that individuals have a right to request images of themselves by making a subject access request and the procedure for dealing with requests of this type are covered in Section 5 Annual Assessment of Compliance with the Information Commissioner's Code of Practice.

All members of staff who have access to the stored images will follow these guidelines in the consideration of any access request.

Whilst the organisation does not state in its registration with the Information Commissioner's Office that it is a public authority, it adheres to the guidance for academies on freedom of information issued by the Department for Education. This enables us to comply with data protection and freedom of information principles in the manner of a "relevant authority" as defined by the Protection of Freedoms Act 2012. Requests for information about the CCTV system under the Freedom of Information Act are, therefore, covered by this document.

7.4 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 7

Principle 8

Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

1. *Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focussed on typical CCTV installations. However, there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition system, or where there is a specific deployment scenario, for example the use of body worn video recorders.*

2. *Approved standards are available to inform good practice for the operation of surveillance camera systems, including those developed domestically by the British Standards Institute, at the European level by the Comite Europeen de Normalisation Electrotechnique, or at a global level by the International Electrotechnical Commission. A system operator should consider any approved standards which appear relevant to the effective operation of technology to meet the purpose of their system and taking steps to secure certification against those standards.*

3. *A current list of recommended standards for consideration by a system operator will be maintained and made available by the Surveillance Camera Commissioner. Such a list will provide detailed guidance on suitable standards and the bodies that are able to accredit performance against such standards.*

8.1 Relevant Standards

Installers, maintainers and manufacturers of installed equipment are required to conform to BS EN 62676

8.2 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 8

Principle 9

Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use

1. *Putting effective security safeguards in place helps to ensure the integrity of the images and information, should they be necessary for use as evidence in legal proceedings. This also helps to foster public confidence in system operators and how they approach the handling of images and information.*
2. *Under the 1998 Act, those operating surveillance camera systems, or use or process images and information obtained by such systems must have a clearly defined policy to control how images and information are stored and who has access to them. The use or processing of images and information should be consistent with the purpose for deployment and images should only be used for the stated purpose for which collected.*
3. *Security extends to technical, organisational and physical security and there need to be measure in place to ensure that this is the case and to guard against unauthorised use, access or disclosure. The ICO CCTV Code of practice gives helpful guidance on achieving this in practice.*

9.1 Access to Stored Images

The recording and monitoring equipment is based upon a standalone analogue / IP based system and access is restricted to those individuals identified in section 7.1 above.

9.2 Physical Security

Recording and monitoring equipment is installed in a restricted designated areas and in a position which makes it unlikely that live images could be seen by persons other than authorised users of the system. The equipment is installed in an office which can only be accessed by a code lock. Access can only be gained by the Site Manager and the Site team, or the Operations Director to whom they are accountable as their line manager.

9.3 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 9

Principle 10

There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice and regular reports should be published.

1. *Good practice dictates the system operator should review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose for deployment.*
2. *As part of the regular review of the proportionality and effectiveness of a surveillance camera system, a system operator should assess whether the location of the cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.*
3. *In reviewing the continued use of a surveillance camera system a system operator should consider undertaking an evaluation to enable comparison with alternative interventions with less risk of invading individual privacy and different models of operation (to establish for example 24 hour monitoring). In doing so there should be consideration of an assessment of the future resource requirements for meeting running costs, including staffing, maintenance and repair.*
4. *A system operator should make a summary of such a review available publicly as part of the transparency and accountability for the use and consequences of its operation.*

10.1 Annual Reviews

The date of the next Surveillance Commissioner's Code of Practice Compliance Review will be June 2017. This date has been adjusted to coincide with the annual service and maintenance program which is planned to take place annually in June. This also coincides with the approximate anniversary of the system upgrade.

10.2 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 10

Principle 11

When the use of a surveillance camera system is in pursuit of a legitimate aim and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

1. *The effectiveness of a surveillance camera system will be dependent upon its capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. Wherever the purpose of a system includes crime prevention, detection and investigation, it should be capable through processes, procedures and training of system users, of delivering images and information that is of evidential value to the criminal justice system. Otherwise, the end user of the images, who are likely to be the police and criminal justice system, will not be able to play their part effectively in meeting the intended purpose of the system,.*

2. *It is important that there are effective safeguards in place to ensure the forensic integrity of the recorded images and information and its usefulness for the purpose for which it is intended to be used. Recorded material should be stored in such a way that it maintains the integrity of the image and information, with particular importance attached to ensuring that the metadata (e.g. time, date and location) is recorded reliably and compression of data does not reduce its quality. This is to ensure that the rights of individuals recorded by a surveillance camera system are protected and that the material can be used as evidence in court. To do this the medium on which the images and information are stored will be important and access must be restricted. A record should be kept as an audit trail of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court. Once there is no longer a clearly justifiable reason to retain the recorded images and information, they should be deleted.*
3. *It is important that digital images and other related information can similarly be shared with ease with appropriate law enforcement agencies if this is envisaged when establishing a system. If this interoperability cannot be readily achieved it may undermine the purpose for deploying the system.*
4. *It is therefore essential that any digital images and information like to be shared with law enforcement agencies of the criminal justice system are in a data format that is interoperable and can be readily exported and then stored and analysed without any loss of integrity. In particular;*
    - i. *A system user should be able to export images and information from a surveillance camera system when requested by a law enforcement agency.*
    - ii. *The export of images and information should be possible without interrupting the operation of the system*
    - iii. *The exported images and information should be in a format which is interoperable and can be readily accessed and replayed by a law enforcement agency.*
    - iv. *The exported images and information must preserve the quality of the original recording and any associated metadata (e.g. time, date and location)*

11.1 System Effectiveness

The quality of the images produced by the cameras and stored on the recording equipment are consistent with the quality required to be used for evidential purposes.

11.2 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 11

Principle 12

Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

1. *Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure that underlying data is fit for purpose.*
2. *A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was added to a database.*
3. *There may be occasions when the inclusion of information about an individual in a reference database with the intention of undertaking surveillance can be considered as covert surveillance and thus fall within the bounds of the 2000 Act. Further guidance on the application of the 2000 Act is available in the Home Office statutory covert surveillance and property interference code of practice and from the office of the surveillance commissioners.*

12.1 Reference Databases

No reference databases are deployed in the system.

12.2 ANPR, Biometric Recognition, or Similar Technologies

These systems and technologies are not currently deployed within the system and therefore no reference databases are required for the operation of such technologies.

12.3 Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 12

Section 5
Annual Assessment of Compliance with the Information Commissioner's Code of Practice

General Statement

Mark Hall Academy operates a CCTV surveillance system which conforms to the principles and practicalities of the Data Protection Act 1998. In particular the organisation adheres to the following Data Protection Principles as set out in the Information Commissioner's Code of Practice to help us ensure that the system continues to operate within the law.

Data Protection Principles

1. Personal data shall be 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 met
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, be kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
7. 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.
8. 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 the data subjects in relation to the processing of personal data.

Principle 1

Personal data shall be 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 met

General Statement

Mark Hall Academy operates the CCTV camera system in a manner which meets the requirements of the Data Protection Act 1998. Data is processed in accordance with documented procedures and in such a way that is consistent with the clearly defined objectives for the continued operation of the system.

We believe that the operation of the system continues to be justified, necessary and proportionate and in order to support this view we conduct an annual privacy impact assessment, which is included in Section 6 below. Within the scope of the privacy impact assessment alternative and complimentary options are regularly considered.

Identification of Compliance Issues
No issues have been identified where further action will be required to more fully comply with the requirements of Principle 1

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes

General Statement
Mark Hall Academy operates the CCTV camera system in order to achieve the following objectives;

1. Enhance the personal safety and security of all persons using the site.
2. Reduce the fear of crime or antisocial behaviour
3. The prevention, deterrence, detection and prosecution of crime or antisocial behaviour
4. Support the disciplinary process in the event of crime or antisocial behaviour
5. The protection and security of valuable assets

Identification of Compliance Issues
No issues have been identified where further action will be required to more fully comply with the requirements of Principle 2

Principle 3

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

General Statement
We believe that the operation of the system continues to be justified, necessary and proportionate and in order to support this view we conduct an annual compliance assessment and privacy impact assessment. The privacy impact assessment is published in Section 6 below. Within the scope of the privacy impact assessment alternative and complimentary options are regularly considered.

The equipment is serviced and maintained on a regular basis in order to ensure that it remains fit for the purposes and clearly stated objectives of operating the system.

The recent system upgrade allows configuration by the system operator to ensure that images are not retained for any longer than the agreed retention period before being subject to destruction by data overwrite.

Identification of Compliance Issues
No issues have been identified where further action will be required to more fully comply with the requirements of Principle 3

Principle 4

Personal data shall be accurate and, where necessary, be kept up to date.

General Statement

Personal data is in the form of stored CCTV images and the documented procedures for the processing of personal data and the technical specification of the equipment is sufficient to ensure that such recorded images are of a quality consistent with the clearly stated objective for continued operation of the CCTV system.

Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 4

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

General Statement

The retention period for the recorded images upon completion of the system upgrade has been set to a maximum of 30 days. Personal data is not used for any other purposes than those required to achieve the stated objectives for the continued operation of the system.

Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 5

Principle 6

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

General Statement

All staff who are authorised to access personal data have received training in the recognition and processing of subject access requests.

Identification of Compliance Issues

The following issues have been identified where further action will be required to more fully comply with the requirements of Principle 6

A number of training opportunities were identified in 2015 in terms of technical operation, procedure and compliance awareness.

In order to resolve these issues the following actions have been taken.

Upon completion and commissioning of the system upgrade a new OEM User Manual has been issued to relevant staff and training on the operation of the new system has been provided by the installation contractor.

Relevant codes of practice detailed in this document have been issued to all authorised staff to support and update on the training provided in the operation of the new system.

Principle 7

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.

General Statement

The recording and monitoring equipment is based upon a standalone analogue and IP based system and access is restricted. The recording and monitoring equipment is installed in restricted designated areas and in a position which makes it unlikely that live images could be seen by persons other than authorised users of the system.
The equipment is installed in an office which can only be accessed by a code lock. Access can only be gained by the Site Manager and the Site team, or the Operations Director to whom they are accountable as their line manager.

Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 7

Principle 8

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 the data subjects in relation to the processing of personal data.

General Statement

This Data Controller states that it may sometimes be necessary to transfer personal information overseas. When this is needed all transfers are made in full compliance with the Data Protection Act. However, personal data is not generally transferred to any country or territory outside the European Economic Area and is not generally processed outside of the organisation except when requested for the purpose of investigating or prosecuting a crime by an appropriate law enforcement agency or by order of a Court.

Identification of Compliance Issues

No issues have been identified where further action will be required to more fully comply with the requirements of Principle 8

Section 6
Annual Privacy Impact Assessment

Part 1 Potential Impacts on Privacy

1. The new CCTV system upgrade involves the collection of images of individuals present on site both in the areas surrounding the building or buildings, but inside its perimeter. It involves the collection of images of individuals within the certain areas of the buildings themselves.

   An extension to an existing CCTV installation has the potential to increase the frequency and number of individuals whose images will be captured and stored.

   An equipment upgrade to an existing CCTV installation has the potential to capture a record images of individuals at high resolutions and therefore greater detail than the original installation.
2. The system will designed in such a way that individuals will be compelled to allow images of themselves to be recorded and stored electronically for a specified period of time.
3. Information will not be disclosed to organisations or people who have not previously had access to the information
4. The purpose for which the information is used will not be extended beyond its current use or in a way in which it is not currently used.
5. The project does not involve the use of new technology which might be perceived as privacy intrusive; e.g. biometric or facial recognition.
6. The project will potentially result in decisions, or taking action against individuals which can have a significant impact on them.
7. The information about individuals is not likely to raise privacy concerns or expectations, e.g. health or criminal records or other information which people would consider to be particularly private.
8. The project will not require us to contact individuals in ways which they may find intrusive.

Part 2 Requirement for a Privacy Impact Assessment

Significant changes to the system in respect extending the installation and the upgrade of equipment are in progress. Therefore, we have identified that a PIA represents a structured approach to identifying the risks involved and any measures which might be adopted to mitigate those risks.

In this way we aim to achieve compliance with the Surveillance Camera Commissioner's Code of Practice and mitigate the risk of breaching the Protection of Freedoms Act 2012

This document is published in contemporaneously with the system upgrade and the effective operation and specification of the equipment deployed will ensure that the images captured and stored continue to meet the quality standard required for evidential purposes and is compliant with The Information Commissioner's Code of Practice

A PIA is needed because the continued operation of a CCTV system involves the capture, storage and processing of images of individuals using the site. In addition the system is designed in such a way that individuals will be compelled to provide images of themselves to be recorded and stored electronically for a specified period of time

Part 3 Information Flows

The collection, use and deletion of personal data is detailed in this document and by definition data flows have already been identified. The number of individuals likely to be affected by the project is approximately the same as it was in 2015 and consists of the general population of the academy on a day to day basis.

A standalone analogue / IP CCTV surveillance camera system is deployed by Mark Hall Academy. Images are captured by strategically located cameras and stored on a dedicated NVR's / DVRs. Images are processed in accordance with strict procedures and access is restricted.

In order to ensure that we have identified and addressed the privacy risks, the following have been consulted during all phases of the project;

The Academy Transformation Trust
The Local Governing Body
The Principal
The Operations Director

Part 4 Privacy and Related Risks

Privacy Issue	Risk to Individuals	Compliance Risk	Organisational Risk
Personal data should be processed fairly and lawfully	Personal information may be shared inappropriately or used for purposes other than those for which it was intended	The organisation may be on breach of the Data Protection Act 1998 Principle 1	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Personal data must only be obtained for specified lawful purpose and should not be processed in any way which is incompatible with those purposes	Personal information may be shared inappropriately or used for purposes other than those for which it was intended	The organisation may be on breach of the Data Protection Act 1998 Principle 2	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Personal data must be adequate, relevant and not exceed those purposes for which they are processed	Stored personal information may be excessive, shared inappropriately or used for purposes other than those for which it was intended	The organisation may be on breach of the Data Protection Act 1998 Principle 3	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Personal data must be accurate and kept up to date	Inaccurate, poor quality information may result in unfair decisions being taken about individuals	The organisation may be on breach of the Data Protection Act 1998 Principle 4	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Personal data for specified purposes and must not be retained for any longer than is necessary for that purpose	Personal information may be used for purposes other than those for which it was intended or may be out of date	The organisation may be on breach of the Data Protection Act 1998 Principle 5	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Personal data must be processed in accordance with the rights of data subject under the Act	Rights of individuals to access data about themselves may be infringed	The organisation may be on breach of the Data Protection Act 1998 Principle 6	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Technical and organisational measures must be taken to ensure against unauthorised and unlawful processing, loss, destruction or damage to personal information.	Personal information may be shared inappropriately or used for purposes other than those for which it was intended	The organisation may be on breach of the Data Protection Act 1998 Principle 7	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system
Personal data ,must not be transferred to any country outside the EEA	The rights and freedoms of the individual may not be protected outside this area	The organisation may be on breach of the Data Protection Act 1998 Principle 7	Reputational damaged, costs of defending prosecution, possible fines, asset loss if ordered to discontinue operation of the system

Part 5 Privacy Solutions

Describe the actions which you will take to reduce the risks and any future steps which would be necessary (e.g. the production of new guidance of future security testing for systems)

Risk	Solution	Result	Evaluation
Personal information may be shared inappropriately or used for purposes other than those for which it was intended	Mark Hall Academy will comply with the principles of the Data Protection Act 1998	The risk will be reduced	This has been evaluated as a justified and proportional response
Personal information may be shared inappropriately or used for purposes other than those for which it was intended	Mark Hall Academy has identified clear and specified lawful purposes for the operation of the CCTV and may not be used for any other purpose	The risk will be reduced	This has been evaluated as an adequate and proportional response
Stored personal information may be excessive, shared inappropriately or used for purposes other than those for which it was intended	Mark Hall Academy has specified equipment which is fit for purpose and has specified a retention. Access to data is strictly limited and steps have been taken to ensure the physical security of the data	The risk will be reduced	This has been evaluated as an adequate and proportionate response
Inaccurate, poor quality information may result in unfair decisions being taken about individuals	Mark Hall Academy has specified equipment which is fit for purpose	The risk will be eliminated	This has been evaluated as a proportional response
Personal information may be used for purposes other than those for which it was intended or may be out of date	Mark Hall Academy has specified a retention period which precludes excessive amounts of data about individuals being retained for longer than is necessary to achieve the lawful purpose and objectives of operating the CCTV system	The risk will be eliminated	This has been evaluated as an adequate response
Rights of individuals to access data about themselves may be infringed	Mark Hall Academy is subject to the provisions of the Data Protect Act 1998 and to the provisions of the Freedom of Information Act 2000	The risk will be reduced	This has been evaluated as a justified and proportional response
Personal information may be shared inappropriately or used for purposes other than those for which it was intended	Access to data is strictly limited and steps have been taken to ensure the physical security of the data	The risk will be reduced	This has been evaluated as an adequate response
The rights and freedoms of the individual may not be protected outside this area	Data may be processed in countries outside the EEA. When this is necessary, transfers will be made in full compliance to the data Protection Act	The risk will be reduced	This has been evaluated as an adequate response

Part 6 Privacy Impact Assessment Outcomes

The following table has been left blank intentionally as this section of the document is for completion by the client.

Who has approved the privacy risks involved in the project and what solutions will need to be implemented?

Risk	Approved Solution	Approved by

Part 7 Project Integration of Privacy Impact Assessment Outcomes

The following table has been left blank intentionally as this section of the document is for completion by the client.

Designate of the person or persons responsible for integrating the PIA outcomes back into the project plan, updating project management documentation as required and implementing the approved solutions. Designate the person / contact point for any privacy concerns which may arise in the future.

Action	Target Date	Person Responsible

Section 7
Compliance Report

Following our review we would advise you that upon completion in May 2016 of the CCTV system upgrade as installed to specification and operated, fully meets the required standards recommended in the Information Commissioner's Code of Practice and the Surveillance Camera Commissioner's Code of Practice.

End of Report