HOLLINGWORTH LEARNING TRUST

CCTV POLICY & PROCEDURES
HOLLINGWORTH LEARNING TRUST

Created:	Autumn 2023
Created By:	S Collinge and J Ward
Approved By:	COO & CEO
Implementation Date:	Summer 2024
Review Date	**To be reviewed by COO every 3 years** Or to be updated as and when new advice and guidance is received regarding Data Protection, Human Rights Act or Surveillance Code of Practice.
Review Body:	COO & CEO

VERSION INFORMATION

Version	Reason for Update	Author	Date	Approved By:
1	Original Policy	S Collinge J Ward	Summer 2023	COO 12.07.2023
2	Policy Update: Access requests to CCTV Use of Bodycam/CCTV audio	S Collinge J Ward	Summer 2024	CEO & COO 08.05.2024

Contents

1. Aim

Hollingworth Learning Trust's ("the Trust") mission is to make a positive difference to the lives of the children in our schools. To deliver this mission, Hollingworth Learning Trust aims to protect the health and safety of pupils, staff and visitors.

This policy sets out the approach to the use of CCTV within Hollingworth Learning Trust. This policy must be followed by all schools within the Trust family.

The aim of this policy is to provide guidance on the management, operation and use of closed-circuit television (CCTV) at Hollingworth Learning Trust.

This is a Hollingworth Learning Trust policy and will be used by all schools within our Trust family. The policy is written for use by individual schools, however, is also applicable to staff employed centrally within the Trust.

This is a non-contractual policy; the policy applies to all staff.

Equality and Diversity Policy Statement:

Hollingworth Learning Trust are committed to meeting our obligations under the Public Sector Equality Duty (PSED) and within our CCTV Policy processes we actively;

- promote equality, diversity and inclusion;
- aim to eliminate discrimination;
- take account of disabilities in any staffing matters.

Trust Vision and Values:

The Trust is committed to ensuring the protection of the health and safety of all our stakeholders, and that by achieving this at every level of the organisation, we aim to embody the Trust core values:

AMBITIOUS:	We have high expectations for all of our children and staff. They deserve the best we can do.
POSITIVE:	We believe that people and schools can improve; we always believe this.
RESILIENT:	We make long term commitments to pupils, families, communities and schools. We never give up.
REFLECTIVE:	We constantly evaluate what we do in order to improve. We are never complacent.
PRINCIPLED:	We always promote equity, equality and challenge injustice. We consistently act in the 'best interests' of our pupils.

2. Introduction

The system comprises of several cameras located at each trust site. All cameras are monitored via access to secure services and are only available to selected authorised users within the academy, Trust and, where applicable, Facilities Management (FM) provider.

2.1 This policy follows Data Protection guidelines and the Information Commissioners Office CCTV Code of Practice (2015).

2.2 This policy will be reviewed every three years or when new advice and guidance is updated.

2.3 This policy meets the requirements of:

- The ICO's Code of Practice for the use of surveillance cameras and personal information.

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020.
- Data Protection Act 2018 (DPA 2018).

2.4 The below table details the ownership, management, and administration of the CCTV systems at Trust sites:

Trust Site	Security CCTV	Behaviour CCTV	Safeguarding CCTV
Hollingworth Academy	Owned by Delmore Equity and managed by the academy's FM contractor, currently EQUANS.	Owned and managed by the academy. Hollingworth Learning Trust administrate on the school's behalf.	Owned and managed by the academy. Hollingworth Learning Trust administrate on the school's behalf.
Newhouse Academy	Owned and managed by the academy.	Owned and managed by the academy. Hollingworth Learning Trust administrate on the school's behalf.	Owned and managed by the academy. Hollingworth Learning Trust administrate on the school's behalf.

3. Objectives of the CCTV scheme

CCTV is used in our academies to:

- Assist in protecting the health and safety of pupils, staff and visitors.
- To assist the academy in safeguarding and pastoral care matters.
- Monitor the security of the premises and the property of the academy, its pupils, staff, and visitors.
- Detect and investigate disciplinary offences which are described in the academy's disciplinary procedures.
- Identify individuals who breach academy policies.
- Assist in the management of the academy premises.

The CCTV system may also be used to investigate complaints and to assist in civil/legal proceedings.

The academy system is not proactively monitored. Classroom, office, and workroom CCTV cameras do not possess live view and can only be used to view recorded footage.

The system will only be used in a manner which is fair to everyone.

4. Statement of intent

4.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act and will seek to comply with the requirements of the Data Protection Act, GDPR and the Commissioner's Code of Practice.

4.2 The academy will treat the system and all information, documents and recordings obtained and used as data which is protected by the Data Protection Act.

4.3 Cameras will be used to monitor activities within the academy, its car parks and other public areas to identify criminal activity, and for the purpose of securing the safety and wellbeing of the academy, together with its visitors.

4.4 The academies and, where applicable, the FM provider, have been instructed that static cameras are not to focus on private homes, gardens, and other areas of private property.

4.5 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property, or a specific group of individuals, without authorisation being obtained, as set out in the Regulation of Investigatory Power Act 2000.

4.6 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and

with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

4.7 The planning and design of the system has endeavored to ensure that the CCTV 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.

4.8 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 academy CCTV.

4.9 The use of audio recording via CCTV is not in operation at sites within the Trust.
The use of audio recording via body worn videos may be in use in specific areas of the Trust. Where this is the case, signage will be displayed, or people will be informed prior to use. For further information about the use of audio recording and body worn videos, please see section 5.4 of this document.

4.10 ANPR is implemented to meet Safeguarding standards, recording vehicle movement on the car parks of certain academy sites and to facilitate the automated barrier for members of staff. The ANPR logs are kept for a period of three months and then deleted.

5. CCTV Systems in the Academy

5.1 Security System

5.1.1 The security CCTV system will be used to monitor activities within the academy, its car parks, and other public areas to identify criminal activity, and for the purpose of securing the safety and wellbeing of the academy, together with its visitors.

5.1.2 Only authorised trust and academy staff will have access to the security system.

5.1.3 Staff using this system will receive training and will be required to complete the CCTV user's form (**Appendix 1**).

5.1.4 At academy PFI sites the Security CCTV may be a shared system. The Trust and academy will share this policy and guidance with the FM provider, requesting that the same management and operations are in place to maintain safe use of the system.

5.2 Behaviour System

5.2.1 The behaviour CCTV system will be used to monitor activities within the academy to identify behavioural issues.

5.2.2 Only authorised academy staff will have access to the behaviour system.

5.2.3 Staff using this system will receive training and will be required to complete the 'CCTV Users' form (**Appendix 1**).

5.3 Safeguarding system

5.3.1 The Safeguarding CCTV system is in place to safeguard pupils, staff, and visitors.

5.3.2 Safeguarding CCTV cameras include those in non-public places, including classrooms, offices, and workrooms.

5.3.3 The Safeguarding CCTV system will only be used when a safeguarding complaint or concern is raised with the academy.

5.3.4 The Safeguarding CCTV system does not possess a live view and can only be used to view recorded footage when a safeguarding complaint or concern is raised.

5.3.5 Only the Trust IT Manager will have access to the Safeguarding CCTV system and only the Headteacher, Deputy Heads or Designated Safeguarding Lead (DSL) can request to view the system, as and when a safeguarding complaint or concern is received.

5.3.6 The safeguarding system will not be used in relation to staff competency.

5.3.7 Where CCTV contains reported indecent images of a child, the DSL will inform the Trust IT Manager immediately with the date, time, and location(s)of the images. The CCTV images must be deleted from the system immediately or as soon as possible. The CCTV images must not be reviewed or downloaded by staff. Review or downloading of such images will lead to disciplinary action and legal proceedings.

5.3.8 The Trust has conducted a Data Protection Impact Assessment for the use of the Safeguarding CCTV system, this is available in **Appendix 8.**

5.4 Audio Recording & Body Worn Videos

5.4.1 To assist in protecting the health and safety of pupils, staff and visitors, the Trust allows for the use of Body Worn Video (BWV) in our academies.

5.4.2 BWV involves the use of cameras that are worn by a person and are attached onto the front of clothing. These devices are capable of recording both visual and audio information. Our academies will not routinely use body worn cameras, BWV's will only be used where necessary to satisfy the objectives set out in Section 3 of this policy. BWV will only be used in specific areas of our academies, please contact the relevant academy for further information.

5.4.3 The Senior IT Technicians/relevant member of staff will be responsible for the training of staff to use BWV within the Trust and will monitor the correct use of BWV. All staff who may use a BWV will receive full training and will not be permitted to use the BWV until they have read this policy completed the BWV Users form in **Appendix 2**.

5.4.4 The Trust has conducted a Data Protection Impact Assessment for the use of BWV and this is available in **Appendix 9.**

5.5 Requests to Review CCTV

5.5.1 Only relevant trained staff have access to review CCTV. For audit purposes, and to ensure safe use of CCTV, where CCTV images need to be accessed or reviewed, staff must contact the relevant individual or team in writing, either via email or via the IT Helpdesk, with the reason for review, and the date, time and location of the incident.

5.5.2 Where a download of CCTV is required, staff must submit a request must be put in writing via email to the IT helpdesk for approval by the Trust IT Manager. The request must include the reason for the download, and the date, time and location of the incident. The IT team will save the CCTV images in a secure area. Downloaded CCTV images will be kept for as long as required or for 12 months.

5.5.3 Verbal requests to review or download CCTV images will not be accepted. Further information about requests to access or download CCTV images can be found in **Appendices 3 & 4.**

6. Roles and Responsibilities

6.1 The Trust

The Trust is responsible for the management and compliance of the academy CCTV systems; any complaints or concerns about the academy's CCTV system should be dealt with in line with the Trust's Complaints Procedures.

6.2 The Facilities Management Contractor (PFI sites only):

- Is responsible for the installation and operation of the Security CCTV system in a manner which complies with the CCTV Code of Practice issued by the Office of the Information Commissioner.
- Is responsible for the necessary maintenance and repair of the Security CCTV systems.
- Is responsible for setting user access permissions of FM users to the system.
- Is responsible for the security of the FM CCTV systems.
- Is responsible for receiving requests to view footage on the CCTV system and process these in line with current legislation and Trust procedures.
- Is responsible for providing statistics to the Trust and relevant interested parties with regards to the use of the CCTV system.
- Is responsible for the installation of the CCTV signs.
- Is responsible for the set up and views of the Security CCTV cameras.

6.3 The Trust IT Manager:

- Is responsible for the installation and operation of the CCTV system in a manner which complies

with the CCTV Code of Practice issued by the Office of the Information Commissioner.
- Is responsible for the necessary maintenance and repair of the Trust CCTV systems.
- Is responsible for setting user access permissions of the central service team and academy users to the system.
- Is responsible for the security of the Trust CCTV systems.
- Is responsible for receiving requests to view footage on the CCTV system and process these in line with current legislation and Trust procedures.
- Is responsible for providing statistics to interested parties regarding the use of the CCTV system.

6.4 The Headteacher, Deputy Heads and DSL:
- Are responsible for liaising with the Trust IT Manager when a safeguarding complaint or concern is raised with the academy and access to the Safeguarding CCTV System is required.
- Only the Headteacher, Deputy Heads and DSL can request to view the Safeguarding CCTV system via the Trust IT Manager.
- The Headteacher should ensure that the academy has CCTV logs in place to monitor CCTV activities in school, see section 7.3.4.

6.5 Staff with Access to Recorded Images and use of Body Worn Videos:

All staff with access:
- Must complete the CCTV or BWV User / Acceptable Use Form in **Appendix 1 or 2.**
- Must complete relevant CCTV or BWV Training with the Trust IT Manager or Senior IT Technician/relevant member of staff.
- Must be aware of the procedures which must be followed when accessing the recorded images.
- Must be aware of their responsibilities under the CCTV Code of Practice issued by the Office of the Information Commissioner and be aware of and comply with this CCTV policy.
- Must ensure that access to, and disclosure of, the images recorded by CCTV or BWV is made in accordance with this policy.
- When CCTV or BWV access or download requests are received, staff must follow the guidance set out in section 5 and **Appendix 3** of this policy.

7. Operation of the System

7.1 CCTV

7.1.1 The CCTV system will be administered and managed in accordance with the guiding principles of the Surveillance Code of Practice.

7.1.2 The day-to-day management will be the responsibility of the Trust IT Manager, Senior SLT at each academy, and, on relevant sites, the FM provider.

7.1.3 The CCTV systems will be operated 24 hours a day, every day of the year.

7.1.4 The CCTV system records in a continuous manner. Where certain cameras are motion sensitive, they will stop recording in certain areas when no movement is detected for a period. Cameras will start recording immediately when motion is detected.

7.1.5 The system records images from each camera to an onsite video recorder unless stored separately; the oldest data will be overwritten by new recording after a period of 31 days. CCTV recording will be overwritten after a period of 31 days, which is a duration of time long enough for concerns about security, behavior or safeguarding to be raised.

7.1.6 The Headteacher must accept that CCTV is a computer technology and as such can experience loss or failure. The use of CCTV cannot be a replacement for supervision. ICT support will endeavor to fix/replace any broken systems within the ICT SLA, however, there are situations where this is not feasible and may take longer, for example building mounted cameras can only be replaced when working at height outside of the building is safe, in some cases a 3rd party company is needed to rectify issue.

Where this is required ICT support will inform the academy's behaviour team of the outage.

7.2 Body Worn Video (BWV)

7.2.1 The Use of BWV at Hollingworth Learning Trust will be administered and managed in accordance with the guiding principles of the Surveillance Code of Practice.

7.2.2 BWV will only be used where necessary to satisfy the objectives set out in Section 3 of this policy.

7.2.3 All incidents that involved the use of BWV will be logged, documenting the name of the authorised user, and the date, time, and reason for use. The member of staff wearing the BWV during an incident is responsible for its use, alerting those present that the device is being used, contacting IT for the download or deletion of images from the device, and where the BWV has been used, logging incidents immediately after they have taken place.

7.2.4 Where the use of BWV is required, before recording commences, the authorised user of the BWV will alert those present that the recording will be taking place, stating the following:

- That the recording will be taking place.
- That this will include audio recording.
- When recording commences, the authorised user of the BMV will verbally confirm the following:
  - The recording is taking place.
  - That this includes audio recording.
  - The authorised users name and other colleagues present.
  - The date.
  - The time.
  - The location.
  - The nature of the incident/reason for recording.

7.2.5 The camera shall be aimed at those involved in the incident, and not at third parties who are not involved. Where possible, the user should do their best to ensure that those not involved in the incident are not captured in the recording.

7.2.6 Following an incident, the user of the BWV should email the IT Helpdesk to request, where necessary, the images to be downloaded from the BWV and stored securely, or if images are not required, for the images contained on the device to be deleted. The authorised user is responsible for handing the BWV device to a member of the IT Team on the day of the incident. A device containing recorded images should not be left unattended.

7.2.7 The member of staff wearing the BWV during an incident is responsible for:

- The correct use of the BWV during an incident.
- Alerting those present that the device is being used both before and after recording has started.
- Contacting IT for the download or deletion of images from the device.
- Logging incidents immediately after they have taken place.

7.2.8 BWV should never be used covertly or concealed.

7.2.9 Footage downloaded from a BWV will be retained for 31 days unless required for the purposes of an investigation.

7.3 Internal Requests to Review and Viewing of CCTV and BWV Images

7.3.1 Live viewing of the CCTV system or reviewing of recorded material prior to the production of specific recordings under paragraph 7.3.10, by authorised staff of the academy and others, including the police, will be permitted at all reasonable times. In these circumstances, it will not be possible to obscure the identity of persons not relevant to any investigation. Safeguarding CCTV cameras do not have a live view capacity and recordings can only be accessed when a safeguarding concern or complaint is raised with the academy.

7.3.2 Approved staff must consider the implications of allowing individuals/complainants to view material in this form. Care must be taken to ensure that evidence is not compromised if potential witnesses are to view material.

7.3.3 The CCTV system will log all views, recording and downloads from the CCTV system.

7.3.4 The academy must ensure that CCTV logs are in place to monitor and record CCTV activities:

- Requests to review CCTV: the log will include the name of the requestor, date, time and location of

CCTV being reviewed and the reason for review.

- Access to review Safeguarding CCTV, will be logged by the Trust IT Manager.
- Body Worn Video Log: this will log the use of and downloads from the BWV in school, and should include the name of the BWV user, date and time of use, reason for use, and if images have been downloaded.
- A log of all downloads from the CCTV systems will be kept by the Trust IT Manager.

7.3.5 Only the Trust IT Manager will have authority to download or store images from the CCTV system. All requests to store or download images from the CCTV system will be submitted in writing via the IT Helpdesk, on the specific CCTV request form, to the Trust IT Manager (see **Appendix 3 & 4**). In the Trust IT Managers absence, this responsibility will be delegated to the Trust COO.

7.3.6 The Trust IT Manager has the right to refuse access, viewing and downloading of images from the system, where they believe the objectives of a request are not in line with the CCTV Policy and Procedures and CCTV Code of Practice.

7.3.7 On request from either the Headteacher, Deputy Headteachers or DSL, the Trust IT Manager will save images to a separate medium and will ensure that they have documented:

- The date on which the images were copied from the system.
- At whose request they were copied from the system.
- The filename and location of the copied images. (All requests to be submitted via email to the IT Helpdesk).
- Footage will be encrypted, and the password sent via secure email to the requestor.
- If appropriate, the signature of the collecting police officer or other agent, where relevant.
- Where information is disclosed to another body, such as the police, it is made clear that they are the data controller for that information, and it is their responsibility to comply with the DPA in relation to any further disclosures. When requesting CCTV images, the police should submit an evidence request form that they sign, and the academy retains and files as part of their relevant CCTV log.

7.3.8 CCTV images of staff will only be accessed if there has been a complaint or concern/allegation about a member of staff that may lead to or has led to an investigation regarding the member of staff. Where there is an investigation, the member of staff will be shown the footage as part of the investigatory process. Where the concern/allegation relates to safeguarding, the CCTV may be shared with external agencies (e.g. LADO, police) in line with KCSIE.

7.3.9 After 31 days, unless it is required as evidence by the police or internal disciplinary or civil proceedings, the requestor of the footage will ensure that the footage is destroyed. If the footage is passed onto a third party, then the destruction of the footage when no longer required is passed onto the requestor.

7.3.10 The academy may release recordings to the police, or other authorised persons, for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, or in other circumstances where the academy is legally obliged to do so, in accordance with the specified purposes of the CCTV system. The academy will form a judgement as to whether releasing recordings which contain images of individuals not relevant to any investigation or request for access may be prejudicial to those individuals, and act accordingly.

7.3.11 The academy may release the identity of individuals on the recording whose presence is relevant to the investigation, or request consent from the individual to disclose their identity. Identity may be disclosed even if this consent is refused when deemed reasonable to do so in the circumstances.

7.3.12 The reason for disclosing copies of the images must be compatible with the reason or purpose for which they were originally obtained.

7.3.13 Requests to review CCTV must be in line with Section 5 of this policy and reviewed by authorised members of staff only.

7.3.14 IT staff will review Security and Behavior CCTV systems under the direction of the Trust IT Manager, where a helpdesk ticket has been submitted and a General CCTV request form (**Appendix 6**) has been completed.

7.3.15 Only the Trust IT Manager will review Safeguarding CCTV and only the Headteacher, Deputy Heads or Designated Safeguarding Lead (DSL) can request to view the system, as and when a safeguarding complaint or concern is received. A helpdesk ticket must be submitted, and a Safeguarding CCTV

request form (**Appendix 5**) completed.

8. Requests from Data Subjects and Others for Access

8.1 Any individual whose personal data is held by the academy in the form of a CCTV or BWV recording can request access to that recording, and the Trust will respond in accordance with the Data Protection Act 2018/General Data Protection Regulation.

8.2 Requests for Data Subject Access should be made to the Trust DPO at Hollingworth Learning Trust.

8.3 Recordings will be released for reviewing to other persons, i.e. not the individual whose personal data it is, in accordance with the General Data Protection Regulation on the authority of the Headteacher, Deputy Headteacher and Designated Safeguarding Lead who must be satisfied of the need to release them, unless ordered to do so under statutory powers.

8.4 The Headteacher will decide whether to allow requests for access by third parties in accordance with academy disclosure policies and CCTV Legislation.

8.5 All requests for access or disclosure should be recorded. If access or disclosure is denied, the reason should be documented. This information will be recorded in the CCTV log.

8.6 The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

8.7 Viewing of the recorded images should take place in a restricted area, for example, in a designated member of staff's office. Other employees, pupils and members of the public should not be allowed to have access to that area when a viewing is taking place.

8.8 Removal of the medium on which images are recorded, or the transfer of images to a portable electronic device for viewing purposes, should be documented as follows:

- The date and time of removal.
- The name of the person removing the images.
- The name(s) of the person(s) viewing the images. If this should include third parties, this should include the organisation of that third party.
- The reason for the viewing.
- The outcome, if any, of the viewing.
- The date and time the images were returned to the system or secure place if they have been retained for evidential purposes.
- Needs encrypting.

8.9 Recordings may be viewed by the police for the prevention and detection of crime or for supervisory purposes.

8.10 A record will be maintained of the release of media to the police or other authorised applicants. A register will be available for this purpose. Viewing of recordings by the Police must be recorded on the CCTV log. Requests by the police can only be made under the Data Protection Act.

8.11 Should a recording be required as evidence, a copy may be released to the police under the procedures described in paragraph 7.3.7, 7.3.10 and 8.7 of this guidance. Media will only be released to the police on the clear understanding that the media and information are to be treated in accordance with this CoP. The academy also retains the right to refuse permission for the police to pass to any other person, the media or any part of the information contained thereon.

8.12 The police may require the academy to retain the stored media for possible use as evidence in the future. Such media will be properly indexed and properly and securely stored until it is needed by the police.

9. Location of Cameras

9.1 CCTV cameras will be sited so that it only monitors areas which are required to be covered by the Headteacher and Senior Leadership Team.

9.2 If cameras are adjustable by operators, they should be restricted so that operators cannot adjust or manipulate them to overlook areas not specified in 9.1.

10. Signage

10.1 Signs will be placed so that staff, students, and the public are aware that they are entering a zone which is covered by surveillance equipment. The signs should be clearly visible and legible.

10.2 The signs will contain the following information:

- Hollingworth Learning Trust, the academy and where applicable, FM Providers, as the organisations responsible for the scheme.
- The purposes of the scheme.
- Details of whom to contact regarding the scheme.
- Hollingworth Learning Trust, the academy and where applicable, FM Providers, will be responsible for the installation of CCTV signage and the replacement of any damaged or missing signage.
- Smaller signs will be placed on the door of any classroom or staff area where CCTV recording is taking place.

11. Security

11.1 Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees. This security is extended to any mobile devices which also have access to the academy CCTV system, this includes being mindful that the device should not be operated by anyone other than the asset guardian of the device.

11.2 Access to the recorded images will be restricted to designated staff who need to have access in order to achieve the purpose of using the equipment.

11.3 All trust and academy employees with access to CCTV images will be aware of the restrictions set out in this policy in relation to access to, and disclosure of, recorded images.

11.4 Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances and, with the consent of the Trust IT Manager, acting in the Headteacher's discretion.

11.5 If access to, or disclosure of the images is allowed, then the following should be documented:

- The date and time at which access was allowed or the date on which disclosure was made.
- The identification of any third party who was allowed access or to whom disclosure was made.
- The reason for allowing access or disclosure.
- The extent of the information to which access was allowed or which was disclosed.

11.6 Recorded images should not be made more widely available. They should not be made available to the media or placed on the internet.

11.7 If it is intended that images will be made more widely available, that decision will be made by the Headteacher/Senior Leadership Team. The reason for that decision should be documented.

11.8 If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals not relevant to the disclosure must not be readily identifiable, or their permission for the disclosure must be sought.

12. Breaches of this Policy (including breaches of security)

12.1 Any breach of the policy by academy staff will be initially investigated by the Headteacher, in order for them to take the appropriate disciplinary action.

12.2 Any serious breach of the policy will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

13. Liaison

13.1 A liaison meeting may be held with all bodies involved in the support of this system.

14. Complaints

14.1 Complaints or concerns about the CCTV system should be dealt with in line with the Trust's Complaints Procedures. The Data Protection Officer at dpo@hltrust.co.uk should be made aware of complaints relating to CCTV.

15. Monitoring and Evaluation of the CCTV system and policy

15.1 Performance monitoring, including random operating checks of the CCTV system, may be carried out by the Trust IT Manager, Trust DPO and Trust Chief Operating Officer.

15.2 A CCTV check will be completed annually by the Trust DPO and Trust IT Manager. See **Appendix 7.**

15.3 Responsibility for the monitoring and evaluation of this policy lies with the Headteacher and Trust DPO.

15.4 A copy of the CCTV Code of Practice which sets out the measures which must be adopted to comply with the General Data Protection Regulations is available from the Information Commissioners office website www.ico.org.uk

16. Links to other Policies

This CCTV Policy & Procedures Policy is linked to our:

- Data Protection Policy
- Safeguarding Policy

17. Appendices

1. CCTV User/Acceptable Use Form.
2. Body Worn Video User/Acceptable Use Form.
3. Procedure for Requests to Access or Disclose Images or Recordings.
4. CCTV Flowchart: Requests to Review Images or Recordings.
5. CCTV Request Form: Safeguarding Request Form.
6. CCTV Request Form: General.
7. CCTV Checklist.
8. Data Protection Impact Assessment: Safeguarding CCTV
9. Data Protection Impact Assessment: Body Worn Video

Appendix 1: CCTV User/Acceptable Use Form

Hollingworth Learning Trust

ACCEPTABLE USE OF THE CCTV SYSTEMS AT HOLLINGWORTH LEARNING TRUST

This form is to be completed by staff who will have access to the Trust's CCTV systems

Name:	
Role:	
Location:	

When using the CCTV systems at Hollingworth Learning Trust:

- I will ensure that the use of the CCTV systems is implemented in accordance with the CCTV Policy and procedures at Hollingworth Learning Trust.
- I will carry out CCTV monitoring in line with objectives set out in CCTV Policy and procedures at Hollingworth Learning Trust
- I will ensure that CCTV monitoring at Hollingworth Learning Trust is consistent with the highest standards and protections.
- I understand that I cannot download images or recordings from the CCTV systems, and this is only to be carried out by the academy's Trust IT Manager.
- I understand that monitoring of CCTV at Hollingworth Learning Trust is reactive.
- I understand that live monitoring of CCTV systems at Hollingworth Learning Trust should only be carried out by specific staff.
- I understand that if I receive a request to view CCTV from pupils, parents, visitors or a third party, this request should be passed onto the Trust IT Manager, Trust DPO or Headteacher.
- I understand that, where CCTV images needs storing, downloading, or passing to a third party, the member of staff must email the request and include necessary information to the Trust IT Manager who will complete and log the task.
- I understand that all my access to the CCTV systems at Hollingworth Learning Trust is logged on the system's access register.
- I understand that where I am required/requested to review CCTV, I must log the request on the Academy CCTV Log.
- I understand that failure to follow the CCTV Policy & Procedures for Hollingworth Learning Trust, may lead to disciplinary action.

I confirm that I understand and agree to the above terms	**Yes / No**
I confirm that I have read and understand the Hollingworth Learning Trust CCTV Policy & Procedures document.	**Yes / No**

Signed:

Date:

Appendix 2: Body Worn Video User/Acceptable Use Form

Hollingworth Learning Trust

ACCEPTABLE USE OF THE BODY WORN VIDEO SYSTEMS AT HOLLINGWORTH LEARNING TRUST

This form is to be completed by staff who will have access to the Trust's BWV systems

Name:	
Role:	
Location:	

When using the BWV systems at Hollingworth Learning Trust:

- I will ensure that the use of the BWV systems is implemented in accordance with the CCTV Policy and procedures at Hollingworth Learning Trust.
- I will carry out BWV monitoring in line with objectives set out in CCTV Policy and procedures at Hollingworth Learning Trust.
- I will ensure that BWV monitoring at Hollingworth Learning Trust is consistent with the highest standards and protections.
- I understand that I cannot download images or recordings from the BWV systems, and this is only to be carried out by the academy's Senior IT Technician.
- I understand that monitoring of BWV at Hollingworth Learning Trust is reactive.
- I understand that the use of the BWV will only be used where necessary to satisfy the objectives set out in Section 3 of the CCTV Policy.
- I understand that if I receive a request to view BWV from pupils, parents, visitors or a third party, this request should be passed onto the Trust IT Manager, Trust DPO or Headteacher.
- I understand that, where the BWV has been used, images contained on the BWV must be downloaded by the Senior IT Technician and the BWV cleared by the end of the school day.
- I understand that as the user of the BWV, it is my responsibility to pass the BWV to the Senior IT Technician, to download or clear images in line with the Trust CCTV policy and procedures.
- I understand that I must log the use of the BWV on the required BWV log after use, including the date, time and reason for the recording.
- I understand that failure to follow the CCTV Policy & Procedures for Hollingworth Learning Trust, may lead to disciplinary action.

I confirm that I understand and agree to the above terms	**Yes / No**
I confirm that I have read and understand the Hollingworth Learning Trust CCTV Policy & Procedures document.	**Yes / No**

Signed:

Date:

Appendix 3: CCTV Policy & Procedures: Requests for Images

CCTV System	Information	Actions
Safeguarding CCTV	• Only the Headteacher, Deputy Headteachers or DSL can submit a request to view or download images from the Safeguarding CCTV system. • The Safeguarding CCTV System can only be viewed when a safeguarding concern or complaint is received by the academy. • A 'Safeguarding CCTV Request Form' must be completed and submitted to the Trust IT Manager before images can be viewed. • For matters pertaining to the Headteacher, it would be mandated by the Chair of Governors.	• On receipt of the 'Safeguarding CCTV Request Form' the Trust IT Manager will allow access to the requesting member(s) of the Senior SLT. • Where images need to be downloaded or stored, this will be carried out by the Trust IT Manager in line with the CCTV Policy and the CCTV Code of Practice. • All access, downloads and saving of images from the Safeguarding CCTV system will be recorded on the CCTV log. • After 31 days, unless the images are required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed.
Security & Behaviour CCTV Systems	• Where staff or third parties request to view or access CCTV images a CCTV Request Form must be completed and submitted to the Trust IT Manager.	• On receipt of the 'General CCTV Request Form' the Trust IT Manager/Pastoral/Site Team will review the CCTV and will allow access to the requesting member(s) if necessary. • Where images are to be viewed only, an appointment will be arranged in a restricted area. Other employees, pupils or other persons should not be allowed access to that area when viewing is taking place. • Where images need to be downloaded or stored, this will be carried out by the Trust IT Manager in line with the CCTV Policy and the CCTV Code of Practice. • All access, downloads and saving of images from the CCTV system will be recorded on the CCTV log. • After 31 days, unless the images are required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed.
Body Cam	• When the BWV is used, the member of staff who has used the BWV must log the date, time, reason, and location of use of the BWV. • Images recorded on the BWV must be downloaded by IT Technicians as soon as possible on the day the incident has taken place. Images will be kept for 31 days in line with CCTV policy. • After 31 days, unless the images are required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed. • If a request is received to review BWV images a CCTV request form must be completed and submitted to the Trust IT Manager.	• On receipt of the 'General CCTV Request Form' the Trust IT Manager will review the CCTV and will allow access to the requesting member(s) if necessary. • Where images are to be viewed only, an appointment will be arranged in a restricted area. Other employees, pupils or other persons should not be allowed access to that area when viewing is taking place. • Where downloaded BWV images need to be retained this will be carried out by the Trust IT Manager in line with the CCTV Policy and the CCTV Code of Practice. • All access, downloads and saving of images from the BWV system will be recorded on the BWV log.
Police Requests	• Where the academy receives a request from the police to view or remove images from the academy	• Where images are to be viewed only, an appointment will be arranged in a restricted area. Other employees, pupils

	CCTV system, the relevant CCTV Request Form will be submitted by a member of the Senior SLT to the Trust IT Manager. • CCTV requests from the police must be received, in writing, via an Evidence Request Form which is signed by the investigating officer and filed by the academy in the CCTV log.	or other persons should not be allowed access to that area when viewing is taking place. • Where images need to be downloaded or stored, this will be carried out by the Trust IT Manager in line with the CCTV Policy and the CCTV Code of Practice. • Where images are sent to the police, images will be stored on specific media, protected in line with the DPA and sent securely with confirmation of receipt recorded on the CCTV log. • All access, downloads and saving of images from the CCTV system will be recorded on the CCTV log. • After 31 days, unless the images are required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed.
Subject Access Requests	• Where the Trust or academy receives a subject access request in relation to the academy CCTV systems, this will be sent onto the Trust DPO to review.	• The DPO will review each CCTV access request in line with DPA and whether it is appropriate to share the images. • The Trust and academy have the discretion to refuse any request for information unless there is an overriding legal obligation. • Refusal to disclose information will be recorded on the CCTV log. • Where access to CCTV is granted, the DPO will submit a CCTV Request Form to the Trust IT Manager. • Where images are to be viewed only, an appointment will be arranged in a restricted area. Other employees, pupils or other persons should not be allowed access to that area when viewing is taking place. • Where images need to be downloaded or stored, this will be carried out by the Trust IT Manager in line with the CCTV policy and the CCTV Code of Practice. • To ensure the rights and protections of others in the images, the academy will consider: – The risk and safety of others in the images. – Whether identifying features of others in the footage needs to be obscured. • All access, downloads and saving of images from the CCTV system will be recorded on the CCTV log. • After 31 days, unless the images are required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed.

Appendix 4: CCTV Flowchart

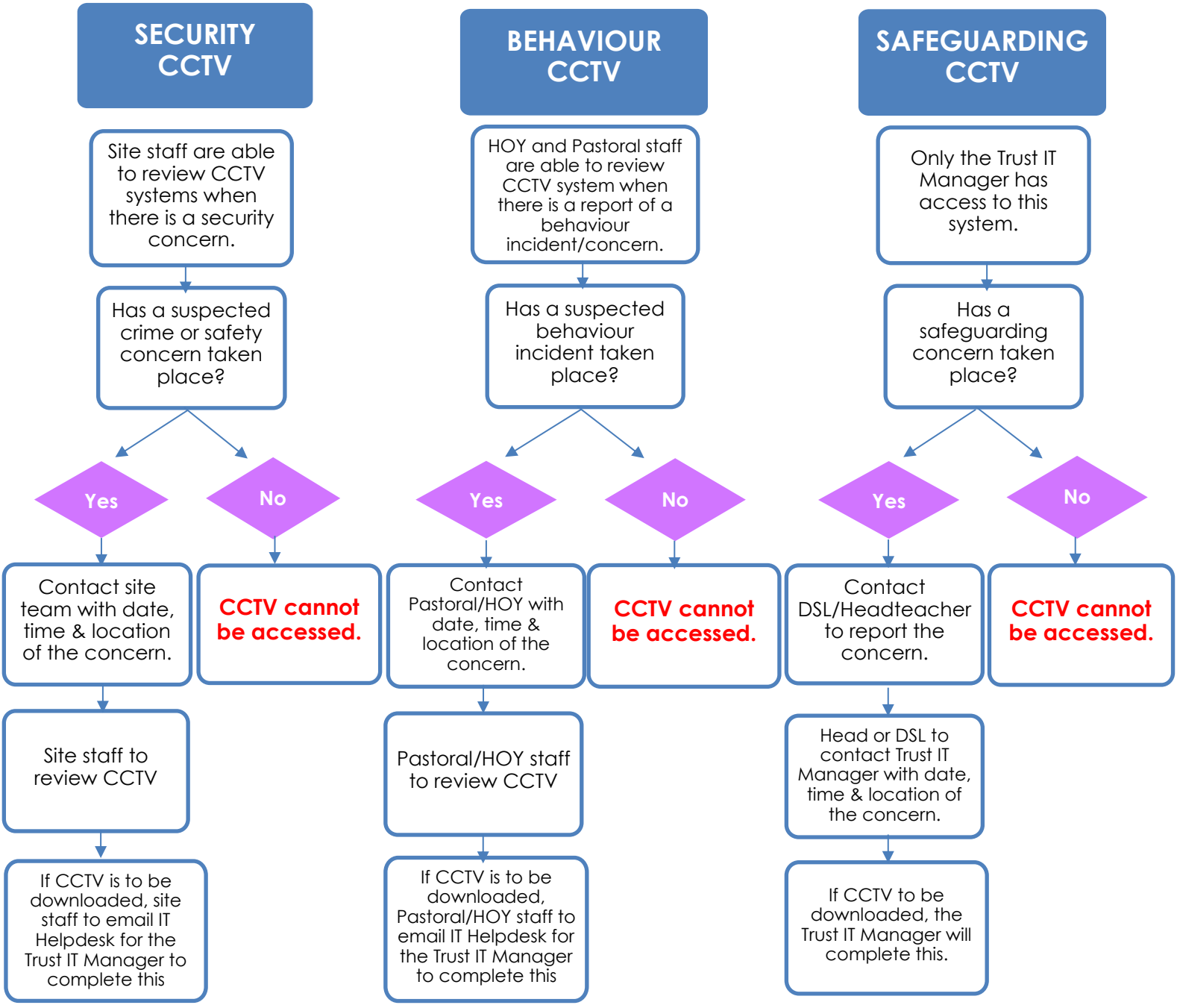
Where CCTV needs to be reviewed, staff must contact the relevant teams or individuals.

Where CCTV needs to be removed, staff must submit a request via the IT Helpdesk along with a General CCTV Request Form or a Safeguarding Request Form (see **Appendix 4 and 5**).

All CCTV access requests must be submitted in writing. Verbal requests will not be accepted.

ONLY AUTHORISED STAFF SHOULD REVIEW CCTV SYSTEMS

CCTV images of staff will only be accessed if there has been a complaint/concern submitted about a staff member that may, or has, led to an investigation. These requests must be submitted by the Headteacher or HR.



Where CCTV contains indecent images of a child, the Trust IT Manager will delete CCTV footage immediately WITHOUT REVIEW OF THE IMAGES. The DSL will inform the Trust IT Manager immediately with the date, time and location of the incident.

Appendix 5: CCTV Policy & Procedures: Safeguarding CCTV Request Form

Hollingworth Learning Trust

CCTV Policy & Procedures: Safeguarding CCTV Request Form

Viewing of the Safeguarding CCTV is limited to Senior SLT only - The Headteacher, Deputy Headteachers and the DSL. The Trust IT Manager will facilitate the requests to access the system.
The Safeguarding CCTV system can only be accessed when a safeguarding concern or complaint is received by the academy.

Removal or downloading of images from the Safeguarding CCTV System can only be carried out by the Trust IT Manager.
The Trust IT Manager has the right to refuse access, viewing and downloading of images to the system, where they believe the objectives of the request are not in line with the CCTV Policy and Procedures and CCTV Code of Practice.

Name		
Role		
Date of Request		
Reason for the Request		
Request Approved?		
Reason for Refusal	*Where requests are refused a reason must be given*	
Name and Role of Persons viewing the CCTV *Where third party persons, i.e the police, are viewing the CCTV, this must be approved by the Headteacher*		
Name	**Role**	**Headteacher Approved**
Date and Time of Images to be viewed		
Location of Camera(s)		

Images Viewed	

Removal or Downloading of Images from the Safeguarding CCTV System

Date and Time of Removal of Images from the CCTV System	
Name of Person Removing the Images	
Reason for Removal of Images	
Images being Removed (including date, times, and camera locations)	
Saved Location of Removed Images	
How long do Images need to be saved for?	
After 31 days, unless the images are required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed.	
Images have been stored in a secure designated area on the academy system.	**Yes / No**
Images that have been downloaded from the academy systems, have been encrypted, password protected onto secure media.	**Yes / No**
Where images are being given to the police, a signed evidence slip has been submitted by the Investigating Officer and filed with the CCTV log.	**Yes / No**

Appendix 6: CCTV Policy & Procedures: General CCTV Request Form

Hollingworth Learning Trust

CCTV Policy & Procedures: General CCTV Request Form

Access to the academy's Security and Behaviour CCTV Systems is limited to authorised staff only. This includes:

- Headteacher,
- Deputy Headteachers & Senior Leadership Team
- Designated Safeguarding Lead
- Head of Years
- Trust IT Manager
- Trust COO and DPO
- Academy Site or Facilities Management Provider *(Security CCTV System Only)*

Removal or downloading of Images from the Security or Behaviour CCTV Systems can only be carried out by the Trust IT Manager.

The Trust IT Manager has the right to refuse access, viewing and downloading of images to the system, where they believe the objectives of the request are not in line with the CCTV Policy and Procedures and CCTV Code of Practice.

Name	
Role	
Date of Request	
Reason for the Request	
Request Approved?	
Reason for Refusal	*Where requests are refused a reason must be given*

Name and Role of Persons viewing the CCTV *Where third party persons, i.e the police, are viewing the CCTV, this must be approved by the Headteacher*		
Name	**Role**	**Headteacher Approved**
Date and Time of Images to be viewed		

Location of Camera(s)	
Images Viewed	

Removal or Downloading of Images from the Behaviour or Security CCTV System

Date and Time of Removal of Images from the CCTV System	
Name of Person Removing the Images	
Reason for Removal of Images	
Images being Removed (including date, times, and camera locations)	
Saved Location of Removed Images	
How long do Images need to be saved for	
After 31 days, unless the images required as evidence in police or internal disciplinary or civil proceedings, the footage will be destroyed.	
Images have been stored in a secure designated area on the academy system	**Yes / No**
Images that have been downloaded from the academy systems, have been encrypted, password protected onto secure media	**Yes / No**
Where images are being given to the police, a signed evidence slip have been submitted by the Investigating Officer and filed with the CCTV log?	**Yes / No**

Appendix 7: ICO Checklist for users of limited CCTV systems

Hollingworth Learning Trust

ICO Checklist for users of limited CCTV systems

This CCTV system, and the images produced by it, are controlled by Hollingworth Learning Trust, Hollingworth Academy, Newhouse Academy and EQUANS Facilities Management, who are responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998.1)

We, Hollingworth Learning Trust, Hollingworth Academy and Newhouse Academy have considered the need for using CCTV and have decided it is required:

- To assist in protecting the health and safety of pupils, staff and visitors.
- To assist the academy in safeguarding and pastoral care matters.
- To monitor the security of the premises and the property of the academy, its students, staff and visitors.
- To detect and investigate disciplinary offences which are described in the academy's disciplinary procedures.
- To identify individuals who breach academy policies.
- To assist in the management of the academy premises.

It will not be used for other purposes.

We conduct an annual review of our use of CCTV.

	Date Checked	By	Date of Next Review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system, when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			

The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

A copy of this checklist will be saved with the CCTV Log until the date of the next review.

Appendix 8: Data Protection Impact Assessment: Safeguarding CCTV

SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

Data protection impact assessments template for carrying out a data protection impact assessment on surveillance camera systems

Project name: Safeguarding CCTV

Data controller(s): Hollingworth Learning Trust

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☒ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☒ Targeting children / vulnerable adults
☒ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

This is for an expansion of the current CCTV to include the use of CCTV in classrooms, workrooms and offices.
The Trust will be processing under UKGDPR.
The classroom CCTV will not be in use until Autumn 2023 at the earliest.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

The school is adding safeguarding CCTV to their current system. The following has been put in place Safeguard CCTV system:
- The Safeguarding CCTV system is in place to safeguard pupils, staff and visitors.
- Safeguarding CCTV cameras include those in non-public places, including classrooms, offices, and workrooms.
- The Safeguarding CCTV system will only be used when a safeguarding complaint or concern is raised within the academy.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

- The safeguarding CCTV system does not possess a live view and can only be used to view recorded footage when a safeguarding complaint or concern is raised.

- Only the Trust IT Manager will have access to the safeguarding CCTV system and only the Headteacher, Deputy Heads or Designated Safeguarding Lead (DSL) can request to view the system as and when a safeguarding complaint or concern is received.
- The safeguarding system will not be used in relation to staff competency.
Although the school will only use the system for the what is outlined above, this does not affect the right of the subject requesting access to the CCTV under article 15 of UK GDPR,however, where footage is sought, digital images of other users will be obscured to safeguard their idenities.

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

The CCTV will record digital images of Staff, Pupils, and visitors to the school when they are in the academy building and external areas of the school site.
These images will only be viewed when the school has concerns regarding security, behaviour or safeguarding.
Only specific staff will have access to the security systems in school, and these staff will receive full training regarding the use of these systems.
CCTV recordings will be kept for a period of 31 days, which is a duration of time long enough for any concerns about security, behaviour or safeguarding to be raised. After this time the images will be deleted.
CCTV images will only be removed from the system if they meet the criteia set out in the CCTV Act 2018.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

At Hollingworth Academy, the Security CCTV system is owned by Delmore Equity and managed by the academy's FM contractor, currently EQUANS. Equans will only have access to the Security CCTV.
Only specific senior staff at HLT will have access to the behaviour & safeguarding CCTV system. Data from the CCTV systems will not be shared with other organisation or agencies unless they meet legal requirements.

6. How is information collected? (tick multiple options if necessary)

- ☒ Fixed CCTV (networked)
- ☒ ANPR
- ☒ Stand-alone cameras
- ☐ Body Worn Video
- ☐ Unmanned aerial systems (drones)
- ☐ Redeployable CCTV
- ☐ Other (please specify)

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

Image recorded (No Audio)
Image retained for period of 30 days
Image destroyed

If the image was to be removed from the system, this would be saved into a secure area for an additional period of 30 days and subject to destruction unless there is a legal requirement to save the footage.

If footage is passed onto a 3rd party, the reason and purpose will be documented. Media will be encrypted. It is then the 3rd party's responsibility to follow the rules and regulations with regard to retention and destruction.

Only specific senior trust staff can download images from the CCTV system, on site staff do not have access to the system.

8. Does the system's technology enable recording?

- ☒ Yes
- ☐ No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Undertaken on the school site - audio is not recorded.
The CCTV system is air gaped and not network connected. No access can be gained from the main ICT systems.

9. If data is being disclosed, how will this be done?

☒ Only by on-site visiting

☐ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)

☐ Off-site from remote server

☐ Other (please specify)

10. How is the information used? (tick multiple options if necessary)

☐ Monitored in real time to detect and respond to unlawful activities

☐ Monitored in real time to track suspicious persons/activity

☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.

☒ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☐ Linked to sensor technology

☒ Used to search for vulnerable persons

☐ Used to search for wanted persons

☒ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies

☐ Recorded data disclosed to authorised agencies to provide intelligence

☒ Other (please specify)

Recorded data reviewed by the school to support investigations regarding security, behaviour and safeguarding incidents in school.
Classroom CCTV only used for safeguarding incidents retrospectively.

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Staff	Survey	Performance Management	Policy states it is not used for staff competency
Unions	Survey	Performance Management	Policy states not for staff competency

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

Public Task:
CCTV is in operation for the purpose of:
- Assist in protecting the health and safety of our pupils, staff and visitors.
- To assist the academy in safeguarding and pastoral care matters.
- Monitor the security of the premises and the property of the academy, its pupils, staff and visitors.
- Detect and investigate disciplinary offences which are described in the academy's disciplinary procedures.
- Identify individuals who breach academy policies.
- Assist in the management of the academy premises

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

CCTV Policy
School Privacy Notices
Signage upon entry to the site and building and further signage around the school.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

Use is auditied, strict control of who can use it, restricted access to safeguarding CCTV.

15. How long is data stored? (please state and explain the retention period)

30 days
This period is long enough for issues to be raised regarding behaviour, security and safeguarding.
After this time the data is deleted.

Date and version control: 19 May 2020 v.4

16. Retention Procedure

☒ Data automatically deleted after retention period

☐ System operator required to initiate deletion

☒ Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

Where CCTV is downloaded to investigate an incident, this data will be retained on the schools secure systems with access limited to specific senior staff. Once the investigation has been completed the data will be deleted, or retained for time periods specific to that investigation.

Where copies of CCTV are passed to the police/courts as part of legal/criminal proceedings, the school will no longer have control over how long they retain this data.

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

CCTV is saved on secure systems.
Only approved staff will have access to the CCTV systems
All staff with access will receive training regarding the systems and the lawful processing of the data contained within the system.
All staff with access to the systems will be required to sign the HLT Acceptable Use of CCTV Sytems.
The CCTV system will retain a log of all staff who access the system on the acces register.
Only the Trust IT Manager is able to store, download or pass CCTV images on to third parties, this will be done on a case by case basis for Safeguarding.
Only IT technicians for behaviour/security - this is audited and an official request including purpose needs to be made.
Staff are informed that failure to follow the CCTV policy and procedures may lead to disciplinary action.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

Details for data subjects regarding access to the their data is included in the Trust Data Protection Policy and Privacy notices.
It is recommended that the trust have a procedure in place to respond to request for camera footage in which other subjects appear.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

Other solutions include:
Maglock doors aroung the building
the site it well lit internally and externally.
Cameras are motion sensitive, they do not run continuously.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

☒ The agencies that are granted access

☒ How information is disclosed

☒ How information is handled

Are these procedures made public? ☐ Yes ☒ No

Are there auditing mechanisms? ☒ Yes ☐ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

The reviewed CCTV policy has not yet been made public, this has been through consultation with staff and awaiting final approval. It will then be available on the trust and schools websites.
Access to CCTV footage and requests for saving CCTV footage are fully audited.

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Positioning of CCTV cameras at entrance points to the school and the issue of privacy	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high Low
Ongoing maintenance of CCTV equipment preventing breakdowns, etc	Possible	Significant	Medium
CCTV policies and procedures not in place leading to inconsistencies, etc	Probable	Significant	Medium
Appropriate CCTV signage in place which conforms to industry standards	Possible	Minimal	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Positioning of external CCTV cameras will cover the school property only, it will not overlook residential/properties surrounding the school. CCTV cameras within the building will not cover areas of privacy such as toilet cubicles/changing rooms	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Maintenance programme in place for the CCTV systems. Regular updates	Reduced	Low	Yes
CCTV policy is included in the Trust Policy review and to be reviewed every 3 years, or as legislation changes, whichever is sooner.	Reduced	Low	Yes

Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Signage is in place on entry to the site and building, and also around the buildings. Recommenation that a contact number is added to the CCTV posters?	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes

Appendix 9: Data Protection Impact Assessment: Body Worn Video & Audio Recording

SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

Data protection impact assessments template for carrying out a data protection impact assessment on surveillance camera systems

Project name: Body Worn Camera(BWC)

Data controller(s): Hollingworth Learning Trust

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☒ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☒ Targeting children / vulnerable adults
☒ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

This is the expansion of the current CCTV processes, to include the use of Body Worn Camera in reception areas of schools.
The trust will be processing under UK GDPR.
The Body Worn Cameras will be not in use until Spring / Summer 2024.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

The schools within the trust are including body worn cameras within the current CCTV system:
- The BWC will be put in place for security and to safeguard pupils, staff and visitors.
- The BWC will only be used in reception areas of the school building.
- The BWC is not a continuously recording device, the camera will only be used if/when an incident takes place.
- The footage recorded by a BWC will only be accessed by specific staff following an incident or if a complaint is raised.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

- As the BWC comes under the Security CCTV, the Facilities Manager will have access to the BWC footage and only the Headteacher, Deputy Headteacher(s) or Designated Safeguarding Lead (DSL) can request to view the system following an incident or if a complaint is recevied.

Although the school will only use the system for the what is outlined above, this does not affect the right of the subject requesting access to the CCTV under article 15 of UK GDPR,however, where footage is sought, digital images of other users will be obscured to safeguard their idenities.

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

The CCTV will record digital images of Staff, Pupils, and visitors to the school in the reception area if an incident occurs.
These images will only be viewed when the school has concerns regarding security, behaviour or safeguarding.
Only specific staff will have access to the security systems in school, and these staff will receive full training regarding the use of these systems.
Any recordings on a BWC will be downloaded and stored securely on the school systems by a specific member of staff on the day of the incident. The BWC will be wiped following the download.
Footage removed from the BWC will be kept for a period of up to a year, IT will delete downloaded CCTV images on an annual basis.
CCTV images will only be removed from the system if they meet the criteia set out in the CCTV Act 2018.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

Only specific staff within HLT will have access CCTV system. Data from the CCTV systems will not be shared with other organisations or agencies unless they meet legal requirements.

6. How is information collected? (tick multiple options if necessary)

- ☐ Fixed CCTV (networked)
- ☒ Body Worn Video
- ☐ ANPR
- ☐ Unmanned aerial systems (drones)
- ☐ Stand-alone cameras
- ☐ Redeployable CCTV
- ☐ Other (please specify)

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

The BWC will only be used if and when an incident occurs.
Those who will be captured in the footage will be informed by the user that the BWC is being turned on.
Once recording, those who are being captured in the footage will be informed that the BWV is in use and is recording.
The BWC will record images and audio.
Images will be downloaded from the BWC following an incident and stored securely on the school IT systems.
The BWC will be wiped of images following the download.
If footage is stored, the reason and purpose will be documented.
Only specific staff can download footage from the BWC.
Only specific senior staff can view the images, this is limited to the Headteacher, Deputy Headteacher(s) and DSL.
If footage is passed onto a 3rd party, the reason and purpose will be documented. Media will be encrypted. It is then the 3rd party's responsibility to follow the rules and regulation with regard to retention and destruction.
Footage removed from the BWC will be kept for a period of up to a year, IT will delete downloaded CCTV images on an annual basis.

8. Does the system's technology enable recording?

☒ Yes ☐ No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Non continuous recording - the BWC will only record when activated which will be if an incident occurs.

9. If data is being disclosed, how will this be done?

☒ Only by on-site visiting

☐ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)

☐ Off-site from remote server

☐ Other (please specify)

10. How is the information used? (tick multiple options if necessary)

☐ Monitored in real time to detect and respond to unlawful activities

☐ Monitored in real time to track suspicious persons/activity

☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.

☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☐ Linked to sensor technology

☐ Used to search for vulnerable persons

☐ Used to search for wanted persons

☒ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies

☐ Recorded data disclosed to authorised agencies to provide intelligence

☒ Other (please specify)

Recorded data reviewed by the school to support investigations regarding security, behaviour and safeguarding incidents in school.

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Awaiting confirmation			

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

Public Task:
CCTV and BWC is in operation for the purpose of:
- Assist in protecting the health and safety of our pupils, staff and visitors.
- To assist the academy in safeguarding and pastoral care matters.
- Monitor the security of the premises and the property of the academy, its pupils, staff and visitors.
- Detect and investigate complaints.
- Identify individuals who breach academy policies.
- Assist in the management of the academy premises

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

CCTV Policy
Trust Privacy Notices
Signage upon entry to the site and building
The BWC user will inform those to be captured by the BWC that they will be using the BWC prior to turning on the camera, and will repeat this again when the BWC is in use to confirm it is recording.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

Use is limited to only if an incident is taking place.
Use is audited, strict control of who can use the BWC and access footage.

15. How long is data stored? (please state and explain the retention period)

The BWC will only be used if/when an incident occurs.
Footage removed from the BWC will be kept for a period of up to a year, once footage is not longer required, IT will delete as part of their annual processes.

16. Retention Procedure

☐ Data automatically deleted after retention period

☒ System operator required to initiate deletion

☒ Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

Where CCTV is downloaded to investigate an incident, this data will be retained on the schools secure systems with access limited to specific senior staff. Once the investigation has been completed the data will be deleted, or retained for time periods specific to that investigation.
Where copies of CCTV are passed to the police/courts as part of legal/criminal proceedings, the school will no longer have control over how long they retain this data.

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

CCTV Images are saved on secure systems.
Only approved staff will have access to the CCTV/BWC systems
All staff with access will receive training regarding the systems and the lawful processing of the data contained within the system.
All staff with access to the systems will be required to sign the HLT Acceptable Use of CCTV Sytems.
For BWC - Only the Trust Premises Manager / Trust IT Manager / IT Technicials are able to store and download the images. These images can only be viewed by the Headteacher, Deputy Headteacher(s) and DSL.
Only the Trust IT Manager can pass CCTV images on to third parties, this will be done on a case by case basis for Safeguarding.
Staff are informed that failure to follow the CCTV policy and procedures may lead to disciplinary action.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

Details for data subjects regarding access to the their data is included in the Trust Data Protection Policy and Privacy notices.
It is recommended that the trust have a procedure in place to respond to requests for camera footage in which other subjects appear.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

The Trust has previously used CCTV images, however, following incidents in schools, it is felt audio recording is required in these areas. BWC are a less intrusive method of recording of audio as it does not continuously record, only recording when it is switched on which is limited to if and when an incident occurs.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

☒ The agencies that are granted access

☒ How information is disclosed

☒ How information is handled

Are these procedures made public? ☐ Yes ☒ No

Are there auditing mechanisms? ☒ Yes ☐ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

The reviewed CCTV policy has not yet been made public. It will then be available on the trust and schools websites.
Access to CCTV footage and requests for saving CCTV footage are fully audited.

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Positioning of BWC cameras at entrance points to the school and the issue of privacy	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high Low
Ongoing maintenance of BWC Equipment to prevent breakdown	Possible	Significant	Medium
CCTV and BWC policies and procedures not in place leading to consistencies	Possible	Significant	Medium
Appropriate signage in place which conforms to industry standards	Possible	Minimal	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
CCTV and BWC policies and procedures being forgotten or misfollowed by staff	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Positioning of BWC cameras will cover the reception areas of the schools only, it will not overlook residential/properites surrounding the school. The BWC will only be used if and when an incident is taking place, it will not continuously record footage or audio to respect the privacy of staff, pupils and visitors in this area.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Maintenance programme in place for the CCTV and will be put in place for the BWC, which will include regular updates,	Reduced	Low	Yes
CCTV policy is included in the Trust Policy review and to be reviewed every 3 years, or as legislation changes, whichever is sooner.	Reduced	Low	Yes

Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
CCTV Signage is in place on entry to the site and building, and also around the buildings. As part of procedures, when using the BWC, the user will verbally alert all those within the area where footage is being captured that they are going to use the BWC, and the user will alert all those in the area again when the BWC has commenced recording.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Training on the CCTV and BWC will be carried out with those staff who have access to the systems, this will include the appropriate use of the system and the proceedures that must be followed.	Reduced	Low	Yes