|  |  |
| --- | --- |
| TUDOR PARK EDUCATION TRUST | CCTV Policy |
| Person(s) responsible for updating the policy: | Ndullee Stevens |
| Date Approved: | 2018 |
| Date of Review: |  |
| Status: | To be taken to Directors Nov 2018 |

**CCTV POLICY**

1. **Policy Statement**
   1. The Trust uses Close Circuit Television (“CCTV”) within the premises of the Trust. The purpose of this policy is to set out the position of the Trust as to the management, operation and use of the CCTV at the Trust and in its schools.
   2. This policy applies to all members of our workforce, visitors to the Trust and its school premises and all other persons whose images may be captured by the CCTV system.
   3. This policy takes account of all applicable legislation and guidance, including:
      1. General Data Protection Regulation (“GDPR”)
      2. Data Protection Act 2018 (together the Data Protection Legislation)
      3. CCTV Code of Practice produced by the Information Commissioner
      4. Human Rights Act 1998
   4. This policy sets out the position of the Trust in relation to its use of CCTV.
2. **Purpose of CCTV**
   1. The Trust uses CCTV for the following purposes:
      1. To provide a safe and secure environment for pupils, staff and visitors
      2. To manage entry and exit to the site and buildings
      3. To manage the behaviour of students and investigate any incidents that occur
      4. To prevent the loss of or damage to the Trust buildings and/or assets
      5. To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders
3. **Description of system**
   1. The system comprises 109 cameras. The cameras do not have sound recording capabilities. Logic School cameras are HIKVision 6MP Bullet Network cameras. All other external cameras are HIKVision DS-2CD2763G0-IZS 6 MP IR VF Dome Network cameras. All internal cameras are HIKVision DS-2CD2163G0-I 6 MP IR Fixed Dome Network cameras.

The digital video recording equipment is HIKVision H Series NVR/ DS-96000NI-I16, supporting live view, storage and playback of the connected cameras at up to 12 megapixels resolution.

1. **Siting of Cameras**
   1. All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
   2. Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Trust will make all reasonable efforts to ensure that areas outside of the Trust premises are not recorded.
   3. Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.
   4. Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets. There are no cameras in general classrooms, except the computer rooms.
2. **Privacy Impact Assessment**
   1. Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the Trust to ensure that the proposed installation is compliant with legislation and ICO guidance.
   2. The Trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.
3. **Management and Access**
   1. The CCTV system will be managed by the Finance Director
   2. On a day to day basis the CCTV system will be operated by the site team.
   3. The viewing of live CCTV images will be restricted to senior leaders, reception staff and the site team.
   4. Recorded images which are stored by the CCTV system will be restricted to access by senior leaders and the site team.
   5. No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.
   6. The CCTV system is checked daily by the site team to ensure that it is operating effectively
4. **Storage and Retention of Images**
   1. Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.
   2. Recorded images are stored only for a period of 30 days unless there is a specific purpose for which they are retained for a longer period.
   3. The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
      1. CCTV recording systems being located in restricted access areas;
      2. Screens showing live CCTV images used by reception for the management of entry and exit to the site and buildings, will be sited in such a way as to minimise the risk of inadvertent viewing by others
      3. The CCTV system being encrypted/password protected;
      4. Authorisation must be obtained from the Director of Finance for the removal of data from the CCTV system.
   4. The CCTV system maintains an audit trail whenever any user initiates playback on a camera. This logs the channel (camera) number, the current time and the user that logged in.
   5. In addition, the Trust will maintain a log of any instances whereby images are removed from the system or shown to anyone other than authorised staff.
5. **Disclosure of Images to Data Subjects**
   1. Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.
   2. Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Trust’s Subject Access Request Policy.
   3. When such a request is made the Director of Finance will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.
   4. If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Director of Finance must take appropriate measures to ensure that the footage is restricted in this way.
   5. If the footage contains images of other individuals then the Trust must consider whether:
      1. The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
      2. The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
      3. If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
   6. A record must be kept, and held securely, of all disclosures which sets out:
      1. When the request was made;
      2. The process followed by the Director of Finance in determining whether the images contained third parties;
      3. The considerations as to whether to allow access to those images;
      4. The individuals that were permitted to view the images and when; and
      5. Whether a copy of the images was provided, and if so to whom, when and in what format.

*[Please note that when a subject access request is made then, unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose) then the requester is entitled to a copy in a permanent form. We have referred only to “access” as opposed to a “permanent copy” as the Trust may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided. However if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort.]*

1. **Disclosure of Images to Third Parties**
   1. The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
   2. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
   3. If a request is received form a law enforcement agency for disclosure of CCTV images then Alex Pett must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.
   4. The information above must be recorded in relation to any disclosure.
   5. If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.
2. **Review of Policy and CCTV System**
   1. This policy will be reviewed bi-annually.
   2. The CCTV system and the privacy impact assessment relating to it will be reviewed bi-annually.
3. **Misuse of CCTV systems**
   1. The misuse of CCTV systems could constitute a criminal offence.
   2. Any member of staff who breaches this policy may be subject to disciplinary action.
4. **Complaints relating to this policy**
   1. Any complaints relating to this policy or to the CCTV system operated by the Trust should be made in accordance with the Trust’s Complaints Policy.

**CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE**

1. Who will be captured on CCTV?

|  |
| --- |
| [Pupil Pupils, staff, parents/carers, volunteers, contractors, hirers, governors/directors, other users of the site (e.g. the Rise School, nurseries ec.) and other visitors including members of the public |

1. What personal data will be processed?

|  |
| --- |
| [Facia Facial images, behaviour, vehicle registration numbers |

1. What are the purposes for operating the CCTV system? Set out the problem that the [Trust/Academy/School] is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

|  |
| --- |
| The Trust uses CCTV for the following purposes:   * To provide a safe and secure environment for pupils, staff and visitors * To manage entry and exit to the site and buildings * To manage the behaviour of students and investigate any incidents that occur * To prevent the loss of or damage to the Trust buildings and/or assets * To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders |

1. What is the lawful basis for operating the CCTV system?

|  |
| --- |
| [Legal Legitimate interests of the organisation to safeguard pupils, staff and visitors; maintain health and safety; prevent and investigate pupil behaviour incidents; and to prevent and investigate crime |

1. Who are the named persons responsible for the operation of the system?

|  |
| --- |
| Ndullee Stevens, Director of Finance  Al Alex Pett Director of Teaching and Learning |

1. Describe the CCTV system, including:
   1. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;
   2. siting of the cameras and why such locations were chosen;
   3. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;
   4. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and
   5. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

|  |
| --- |
| The system comprises 109 cameras. The cameras do not have sound recording capabilities. Logic School cameras are HIKVision 6MP Bullet Network cameras. All other external cameras are HIKVision DS-2CD2763G0-IZS 6 MP IR VF Dome Network cameras. All internal cameras are HIKVision DS-2CD2163G0-I 6 MP IR Fixed Dome Network cameras.  The digital video recording equipment is HIKVision H Series NVR/ DS-96000NI-I16, supporting live view, storage and playback of the connected cameras at up to 12 megapixels resolution.   1. The cameras have been chosen to provide clear, colour images in the day, and night imagery when dark, so that the cameras can be used for the purposes for which they are obtained. They are vandal-resistant to prevent tampering. 2. The cameras have been sited internally and externally to provide coverage throughout the site, whilst avoiding, where possible, capturing areas beyond the site boundaries. Internal cameras are primarily located in lobbies, corridors and stairwells. We have purposefully avoided siting cameras in classrooms and offices, in order to afford privacy to staff and students at work. Exceptions include the ICT rooms, where the cameras are in place to safeguard expensive equipment; and some areas used by hirers and known to be “problem areas” such as the gym and main hall. 3. Subject to the exceptions noted in b) above, we have avoided siting cameras in classrooms or offices, in order to afford privacy to staff and students. In addition, there are no cameras in any of the changing rooms or toilets. We have sited external cameras giving consideration to public areas i.e. roads and pavements. Where possible, cameras have been angled away from such areas. Some of our gate cameras do capture images beyond the site boundary but are needed in order to manage entry and exit to the site for safeguarding and security purposes. 4. Signage is located throughout the site to ensure that pupils, staff and visitors are aware of the presence of the cameras. 5. The system does not allow third party data to be redacted. |

1. Set out the details of any sharing with third parties, including processors

|  |
| --- |
| **Disclosure of Images to Data Subjects**  Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.  Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Trust’s Subject Access Request Policy.  When such a request is made the Director of Finance or Director for Teaching and Learning will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.  If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Director of Finance must take appropriate measures to ensure that the footage is restricted in this way.  If the footage contains images of other individuals then the Trust must consider whether:   * The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals; * The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or * If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.   A record must be kept, and held securely, of all disclosures which sets out:   * When the request was made; * The process followed by the Director of Finance in determining whether the images contained third parties; * The considerations as to whether to allow access to those images; * The individuals that were permitted to view the images and when; and * Whether a copy of the images was provided, and if so to whom, when and in what format.   **Disclosure of Images to Third Parties**  The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.  CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.  If a request is received form a law enforcement agency for disclosure of CCTV images then the Director of Learning must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.  The information above must be recorded in relation to any disclosure.  If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required. |

1. Set out the retention period of any recordings, including why those periods have been chosen

|  |
| --- |
| Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.    Recorded images are stored only for a period of 30 days unless there is a specific purpose for which they are retained for a longer period.  30 days allows sufficient time to investigate incidents that may have occurred during school holidays and closure periods. |

1. Set out the security measures in place to ensure that recordings are captured and stored securely

|  |
| --- |
| The security measures in place include:   * CCTV recording systems being located in restricted access areas; * Screens showing live CCTV images used by reception for the management of entry and exit to the site and buildings, being sited in such a way as to minimise the risk of inadvertent viewing by others * The CCTV system being encrypted/password protected; * Authorisation must be obtained from the Director of Finance for the removal of data from the CCTV system. |

1. What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

|  |
| --- |
| * Whether it is fair to record individuals in the way proposed * Risk of the system being accessed unlawfully * Risk of images being viewed inadvertently * Potential data breach risk during any transfer of recordings, or when disclosed to third parties such as the police |

1. What measures are in place to address the risks identified?

|  |
| --- |
| * Clear objectives defined in the CCTV policy * Privacy notices * Recordings kept for no more than 30 days * Careful siting of cameras * Signage * CCTV recording systems located in restricted access areas * Access to the system is password protected * Procedures in place re subject access requests and disclosure of images to third parties |

1. Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

|  |
| --- |
| Parents and Pupils have not been consulted as to the use of the CCTV system. The Policy will be shared with parents and students and comment or feedback considered for future review. |

1. When will this privacy impact assessment be reviewed?

|  |
| --- |
| Bi-annually |

**Approval:**

This assessment was approved by the Data Protection Officer:

DPO ………………………………

Date ……………………………….