Heartlands Community Trust

CCTV Policy

Circulated for consultation:	**N/A**	
Approved By	**Directors Meeting**	**15 July 2018**
Signed	**Simon Garrill** **Chief Executive Officer**	**Jeff Twentyman** **Chair of Directors**

1. Review and approval

1.1 Heartlands Community Trust (the "Trust") is a multi-academy trust (MAT), and Directors have overall responsibility for the policy.

1.2 The Board of Directors have overall responsibility for the policy, and the Chief Executive Officer is responsible for the operation of the policy within the Trust, as well as for the maintenance of a record of concerns raised in accordance with this policy and the outcomes.

1.3 This policy is reviewed every 3 years by the School Leadership Team, and is then ratified by the Trust.

1.4 The policy has been reviewed for the new Data Protection Act 2018 and the General Data Protection Regulation (GDPR), and as part of the Trust's obligations in respect of adopting and considering Privacy by Design and Default[1] in all aspects of what it does. The Data Protection Officer has contributed to the production of this policy, and is involved in every review.

1.5 Trust employees are required to follow this policy, failure of which may lead to disciplinary action.

2. Introduction

a. The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system within the Trust estate (i.e. site and school buildings) – for the purposes of safety and security. The system comprises a number of static cameras located around the school estate. All cameras can be monitored from authorised desktops.

b. The CCTV system and the data is owned by Heartlands Community Trust.

3. Aims of the CCTV system

3.1 The system aims to:

- to provide a safe and secure environment for all school users
- to protect the school buildings and assets of the Trust (e.g. against criminal acts such as vandalism/theft of Trust assets and property; unauthorised entry to the site and buildings)
- to increase personal safety and reduce the fear of crime (e.g. threats to the health, safety and welfare of staff, students and other users)
- to assist in managing the schools (e.g. unacceptable behaviour such as the malicious activation of the fire alarm system; the bullying and intimidation of students by other students in areas away from regular staff supervision)

[1] *Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start*

- to support the police in a bid to deter and detect crime

4. Statement of intent

4.1 The Trust has adopted a range of measures to enhance safety, security and the protection of its assets. These include restricted access, lanyards, asset registers etc. CCTV is one of those measures.

4.2 The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and complies with the requirements both of the Data Protection Act 2018, GDPR and Commissioner's Code of Practice[2] – as well as the Human Rights Act 1998 and Regulatory Investigation Powers Act 2000.

4.3 The Trust will treat the system and all information, documents and recordings obtained and used, as *data* which are protected by the Data Protection Act 2018.

4.4 The Trust cameras:

- are used to monitor activities within the schools and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school and its staff, students and visitors.

- are focused on the school buildings, external areas of the premises and around entrances/exits: the positioning the cameras being based upon a security assessments carried out to identify likely areas of concern. The full list of camera locations across the Trust is available at Annex A of this policy.

4.5 Signs are displayed to notify all users that CCTV is in operation, and a information sign, as required under the Data Protection Act 2018, has been placed on the gate to the school site.

4.6 The knowledge secured as a result of CCTV will not be used for any commercial purpose. Information transferred to DVD (or other appropriate media) will only be used for the investigation of a specific crime or incident. Release to the media would only be allowed with the written authority of the police if this was required by them as part of a police investigation.

5. Images recorded

5.1 The system has been set up to provide good quality images that can be used to fulfil the aim as outlined in Section 3. Every camera records simultaneously and the images are stored on disc.

---

[2] *In the picture: A DP code of practice for surveillance cameras and personal information. ICO v1.2 20170609*

5.2 Routine checks are made to ensure that the system is operating in accordance with the terms of this policy, and that information relating to the recordings (date, time etc) are accurate.

6. Data Controller and Data Processor

6.1 The CCTV system is installed and maintained by the Trust. For the proposes of the Data Protection Act 2108, the Trust is a Data Processor but also remains, at all times, the Data Controller of all information collected on the CCTV system (the Trust is registered with the Information Commissioner's Office [ICO] with registration number ZA023921).

7. Storage, retention and access to CCTV images

7.1 The Trust has specified a retention policy of thirty (30) days. The recorded images (data) are retained on school servers, which are located in a locked facility.

7.2 Only authorised personnel may ask for a download of the recorded images, as designated by the Chief Executive Officer/Head of School/DPO. Should this be required, the School Business Manager (SBM) will provide a download to the relevant senior leader (who is fully conversant with the terms of this policy). The SBM will also ensure that any such download is removed after a period of thirty (30) days, unless otherwise specified by the Data Protection Officer (DPO).

7.3 If a staff member without authorisation is found to be accessing the equipment or footage, this *may* lead to disciplinary action being taken.

8. Subject access requests (SAR)

8.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act 2018. However, the right is not an unfettered right and if the data subject is not the subject of any recording but was *'incidentally included'* in a wider recording, then there may be no right for the data subject to have access to the relevant footage. It may also not be possible to give out a recording if it would breach the rights of another data subject in the recording.

8.2 All requests should be made in writing to the Chief Executive Officer/Head of School, as appropriate, as there will need to be a careful evaluation of whether any particular data subject should have access to particular footage. This will be done in conjunction with the DPO, and individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

8.3 The relevant school will respond to requests within thirty (30) calendar days of receiving the written request, for which there is no fee, unless the request is deemed to be 'manifestly unfounded or excessive'. In instances where the request is particularly complex, two (2) additional months may be granted to comply with ICO. guidance

8.4 The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation, or would otherwise contravene the law.

8.5 Further details regarding how the Trust responds to Subject Access Requests are available within the Trust's Data Protection Policy available on its websites.

9. Access to and disclosure of images to third parties

9.1 There will be no disclosure of recorded data to third parties, other than to authorised personnel such as the police and service providers to the school where they would reasonably need access to the data (e.g. investigators).

9.2 Requests should be made in writing to the Chief Executive Officer/Head of School, and will be managed in conjunction with the DPO (Data Protection Officer).

9.3 The data may be used within the school's disciplinary and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

10. Complaints

10.1 Complaints and enquiries about the operations of CCTV within the school should be directed to the Chief Executive Officer in the first instance. *Such complaints will be dealt with under the terms of the Trust Complaints Policy*, which is published on the school websites, and which is also compliant with the requirements of the Data Protection Act 2018 and the GDPR.

11. Other relevant school policies

11.1 Other relevant trust-wide policies include the *Data Protection Policy, Complaints Policy*.

12. Further information

12.1 Further information on CCTV and its use is available as follows:

- In the picture: A data protection Code of Practice for surveillance cameras and personal information 2017 (published by the Information Commissioner's Office) www.ico.org.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018
- The Protection of Freedoms Act 2012

Annex A

Locations of CCTV cameras at Heartland High School

- Main Office – In between the 2 doors (waiting area)
- Camera 1 - ASD Gate 3
- Camera 2- Central Forum
- Camera 3- Community Entrance Gate
- Camera 4- Car park 1
- Camera 5- Carpark 2
- Camera 6- North Playground
- Camera 7- Gate 1
- Camera 8- Access road
- Camera 9- Bin store 1
- Camera 10- Bin store 2
- Camera 11- Restaurant 1
- Camera 12- awaits central forum 3rd floor exit
- Camera 13- Staircase 4 level 3
- Camera 14- Outside S3.12
- Camera 15- S3.4
- Camera 16- Outside Restaurant Level 3 South
- Camera 17- Restaurant 2
- Camera 18- Restaurant 3
- Camera 19- Stair 2 Level 3
- Camera 20- Level 3 Central forum
- Camera 21- Level 3 Central forum Library
- Camera 22- Staircase 1 Level 3
- Camera 23- Level 3 North
- Camera 24- Outside Facilities Office
- Camera 25- n3.3
- Camera 26- N3.5
- Camera 27- N3.10
- Camera 28 - Stair 3 Level 3
- Camera 29- Stair 4 Level 4
- Camera 30- S4.14
- Camera 31- S4.2
- Camera 32- F4.19
- Camera 33- Stair 2 Level 4
- Camera 34- F5.19
- Camera 35- N4.1 Outside Sports Hall
- Camera 36- N4.3
- Camera 37- N4.9
- Camera 38- Stair 3 Level 2
- Camera 39- Stair 4 Level 5
- Camera 40- S5.9
- Camera 41- S5.3
- Camera 42- Level 5 Boys Toilet
- Camera 43- F5.24
- Camera 44- Stair 2 Level 5
- Camera 45- F4.13

- Camera 46- Stair 1 Level 5
- Camera 47- Level 5 North
- Camera 48- N5.2
- Camera 49- N5.10
- Camera 50- Stair 3 Level 5
- Camera 51- Stair 4 Level 2
- Camera 52- ASD LEVEL 2
- Camera 53- Level 4 North
- Camera 54- Stair 4 Level 1
- Camera 55- ASD Level 1
- Camera 56- Stair 1 Level 1
- Camera 57- Reception
- Camera 58- Central Forum Table Tennis
- Camera 59- Conference room 1
- Camera 60- Conference room 2
- Camera 61- Stair 3 Level 1
- Camera 62- Gate 2 Student Entrance
- Camera 63- Engage
- Camera 64- Grab and Go

Example of CCTV sign outside main entrances