	Vanguard Learning Trust *As a group of local primary and secondary schools, Vanguard Learning Trust's mission is to serve its local community by providing outstanding, inclusive education. We have a collective purpose and responsibility to provide effective teaching, through a curriculum based on equality of opportunity and entitlement that allows our students to shine both in and out of the classroom. Each school in the Trust has its own ethos, which also complements the Trust's vision and values, and the common aspiration that all students can achieve their potential.*

Digital Images CCTV

November 2022-2024

Contents

1. Introduction

Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection Policy and can be found in the Record of Data Processing.

2. Policy

2.1 Hermitage Primary School uses Close Circuit Television ("CCTV") within the premises of the school. The purpose of this policy is to set out the operation, use, storage and disclosure of CCTV at the School.
This policy applies to all data subjects whose image may be captured by the CCTV system. It works in concurrence with the School's Data Protection Policy, Record of Data Processing and Data Retention schedule.
The policy considers applicable legislation and guidance, including but not limited to;

- General Data Protection Regulation (GDPR)
- Data Protection Act (DPA) 2018
- CCTV Code of practice as produced by the Information Commissioner Office (ICO)
- Human Rights Act 1998.

2.2 The CCTV system is owned and operated by Hermitage Primary School and the deployment is determined by the Senior Leadership Team, with consultation from the Board of Governors and Data Protection Officer (DPO).

The school will:

- Notify the ICO of its use of CCTV as part of its registration.
- Complete a Data Privacy Impact Assessment if amendments are to be made to the deployment or use of CCTV.
- Treat the system and all information processed on the CCTV system as data which is processed under DPA 2018/GDPR.
- Not direct cameras outside of school grounds onto private property, an individual, their property or a specific group of individuals. The exception to this would be if authorization was obtained for Direct Surveillance as set up by the Regulatory of Investigatory Power Act 2000.
- Display Warning signs will be positioned clearly in prominent places.
  Specifically, at all external entrances of the school site where CCTV is use and covers external areas. These signs will include information on how to contact the school regarding information or access to the CCTV footage.
- There is no guarantee that this system will or can cover and detect every single incident taking place in the areas of coverage.

2.3 CCTV footage will not be used for any commercial purposes.

3. Data protection

3.1 Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection Policy and can be found in the Record of Data Processing.

4. Camera set up

4.1 The CCTV system is comprised of 21 cameras which record day and night covering the Internal & External areas of the School. Their coverage also extends past the school boundaries to public areas.

4.2 Cameras will be placed so they only capture images relevant for the purposes for which they are installed, and all care will be taken to ensure that reasonable privacy expectations are not violated.

4.3 CCTV is not sited in classrooms and will not be used in such, except in exceptional circumstances.
Members of staff on request can access details of CCTV camera locations.

5. Purpose of CCTV

5.1 The School uses CCTV for the following purposes:

- To provide a safe and secure environment for the workforce and visitors.
- To protect the school buildings and assets.
- To assist in the prevention and detection of criminal activity.
- Assist law enforcement agencies in apprehending suspected offenders.

6. Covert monitoring

6.1 The school retains the right in exceptional circumstances to set up covert monitoring. For example;

- Where there is good course to suspect illegal or serious unauthorized action(s) are taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances' authorisation must be obtained from the Head Teacher and Chair of Governors.

6.2 Covert monitoring will cease following the completion of an investigation.

7. Storage and retention

7.1 Recorded data will not be retained for longer than is necessary, while retained the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of people who images have been recorded.

7.2 All Data will be stored securely;

- The monitor to view CCTV footage will be kept on the Office Reception desk.
- Recordings will be kept for a maximum 30 days on the system. These will be stored on the hard drive.

7.3 The backup policy for footage is for the data associated with an incident to be securely backed up by the Head Teacher.

8. Access to CCTV images

8.1 The ability to view live CCTV footage is only to be provided at the designated location and historical footage by authorised persons once permission has been provided by the Head Teacher with supervision from the Head Teacher, Designated Safeguarding Lead or Deputy Designated Safeguarding Lead.

8.2 Specific live monitoring is limited to the screen on the Office Reception desk monitor.
Direct Access to recorded footage is limited to those given permission by the Head Teacher with supervision from the Head Teacher, Designated Safeguarding Lead or Deputy Designated Safeguarding Lead.

8.3 Only in exceptional circumstances would any other individuals be allowed to view footage, the reasons and details for these circumstances would be recorded for posterity.

9. Disclosure of images to data subjects (subject access requests)

9.1 Any individual recorded in any CCTV image is considered a data subject and therefore has the right to request access to those images.

9.2 These requests will be considered a Subject Access Request and should follow the schools Subject Access Request process.

9.3 Individuals have a right to make a 'subject access request' to access personal information that Hermitage Primary School holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data

- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

9.4 While Hermitage Primary School will comply with the GDPR Regulations and DPA 2018 in regard to dealing with all Subject access requests submitted in any written format, individuals are asked to preferably submit their request by letter, email or fax addressed or marked for the attention of the Data Protection Officer.
They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

9.5 When such a request is made, the footage will be reviewed in accordance with the request. If the footage contains only the data subject making the request, then the individual may be permitted to view the footage. This will be strictly limited to the footage of the data subject making the request and the specific reason for the request. If the footage contains images of other data subjects, then the school will consider if;

- The request requires the disclosure of the images of data subjects other than the requester, and if these additional data subjects can be anonymized from the footage.
- The other individuals in the footage have consented to the disclosure of the images or if their consent could be obtained.
- If not, then either it is reasonable in the circumstances to disclose those images to the data subject making the request.

9.6 The School reserves the right to refuse access to the CCTV footage where this would prejudice the legal rights of other data subjects or jeopardise an ongoing investigation.

10. Disclosure of images to third parties

10.1 The School will only disclose record CCTV footage to third parties where there is a lawful basis to do so.

10.2 Third parties acting on behalf of a data subject will be handled in accordance with the Subject Access Request Policy.
CCTV footage will only be disclosed to law enforcement agencies in line with the purpose for which the CCTV system is in place.

10.3 If a request is received from a law enforcement agency for the disclosure of footage then the school will follow the Subject Access Request process, obtaining the reasoning for wanting to obtain the footage and any data subjects of concern. This will give help enable proper consideration of the extent of what can be disclosed. This information will be treated with the upmost confidentiality.

10.4 If an order is granted by a court for the disclosure of CCTV images then this should be complied with. However, consideration must be given to exactly what the court requires.

10.5 In all instances, if there are any concerns as to what should or should not be disclosed then the DPO should contacted and further legal sought as per requirements.

10. Complaints

10.1 We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer David Coy david.coy@london.anglican.org

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Approval / Revision History

Revision date	By	Summary of Changes Made
November 22	Siobhan Rowland	No changes made, new VLT Policy format applied