Gosford Park Primary School

CCTV POLICY

1. CCTV ADMINISTRATION & THE LAW

1.1 CCTV and its use is governed by the Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR). The School has a legal duty to comply with the relevant Data Protection legislation contained within that Act including the school's use of CCTV in line with data protection legislation. The CCTV Policy should be read in conjunction with the School's additional policies.

1.2 The School is the body that makes the decisions concerning CCTV, for example, who has responsibility for the control of the images, i.e. deciding what is to be recorded, how the images should be used and to whom they may be disclosed. The School is the data controller and is legally responsible for compliance with the GDPR and DPA.

1.3 With regard to the decision as to how the images are used and to whom they may be disclosed, this delegated responsibility lies with the Governing body, SLT and the School's DPO. Certain staff members are identified as authorised personnel, in certain circumstances, regarding the use and control of the equipment and viewing the live or recorded images (see clause 3.1 (f)). This ensures that the sharing of personal data is kept to a minimum within the school.

1.4 CCTV can record personal data in the form of a person's face and may indicate 'special category' personal data, such as a person's ethnic origin or physical disability. This means that live or recorded images and monitor screens should not be viewed by any unauthorised third party, without the consent or knowledge of the data subject, i.e. the person(s) that appear and are identifiable from the footage.

1.5 As an organisation frequented by members of the public, including staff, pupils, parents/carers, visitors and contractors, the School is required to place

CCTV monitors in a secure environment where those members of the public are not able to see images.

1.6 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained by the appropriate person in their responsibilities under the ICO's CCTV Code of Practice. All authorised employees are aware of the restrictions in relation to access to, and disclosure of, recorded images with this CCTV Policy. The School will keep a record of those who have accessed and read the document.

2. WHY THE SCHOOL USES CCTV

2.1 The School uses CCTV for the purpose of a public task duty; the management and security of the site, monitoring health and safety and safeguarding of the pupils, parents, visitors and employees on site. By using CCTV, the School can monitor occurrences on site and also the security of the buildings and grounds. The School may use CCTV for "crime prevention" and it would be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime. The footage may also be used as evidence during internal disciplinary proceedings or complaints where specific issues have been raised and corroborative evidence is necessary.

3. HOW THE SCHOOL USES CCTV

3.1 When installing CCTV there are several issues to be taken into consideration, such as:

a. Where to position the cameras?
b. Where to position the monitors?
c. Who will operate the cameras?
d. Who will handle requests for access to the images?
e. How do we record who sees the images and for what purpose?
f. Who do we authorise to access the images and for what purpose?

a) The person or body responsible for the management of the School's premises, under the guidance of the Data Protection Officer (DPO) will be responsible for identifying the most suitable place to locate the cameras. The CCTV system is owned and operated by the school, and its deployment is determined by the School's management team. The cameras will not process data that may be deemed as 'excessive', such as capturing public areas outside the scope of the School, or where there is a reasonable expectation of privacy such as toilets or staffrooms, as this goes beyond what is proportionate and necessary to fulfil the purpose for processing the personal data.

b) Along with the external considerations, the School's management of premises will identify the most appropriate housing for the monitors, ensuring security and privacy. In maintained schools this may be the

Local Authority. This will take into account the cabling and technical accessories of the equipment. This will be undertaken in compliance with data protection legislation and consideration of the advice taken from the School's DPO.

c) This would need to take into account capturing the best view of buildings for the purposes of security and high risk areas around the School. The School's authorised personnel is responsible for ensuring that the cameras are working correctly and consistently. This may mean retaining the services of a specialist CCTV service company who would be considered authorised personnel.

d) Subject Access Requests are dealt with in a separate clause.

e) A record of access and disclosure will be kept for disclosure of images in accordance with clause 6.

f) Access to recorded images is restricted to authorised personnel only. The images may be subject to disclosure as outlined in clause 7.1.

3.2 The School will conduct a Data Protection Impact Assessment (DPIA) with guidance from the School's DPO in accordance with GDPR, as they are systematically monitoring and capturing 'vulnerable' data subjects, such as children. The School will also ensure a GDPR compliant agreement is in place with any organisation where personal data/CCTV footage is processed on behalf of the School.

3.3 Any changes to CCTV monitoring will be subject to a Data Protection Impact Assessment (DPIA) which will be advised on by the School's DPO.

4. OBJECTIVES OF THE CCTV SYSTEM

4.1 To protect pupils, staff and visitors.

4.2 To increase personal safety and reduce the fear of crime.

4.3 To protect the school buildings and assets.

4.4 Without prejudice, to protect the personal property of pupils, staff and visitors.

4.5 To support the police in preventing and detecting crime.

4.6 To assist in identifying, apprehending and prosecuting offenders.

4.7 To assist in managing the School.

5. STORING AND VIEWING IMAGES

5.1 When conducting a viewing, either of live images or recorded playback, the viewing should take place in a secure office and only those persons who are authorised and/or who appear on the footage, should be present where relevant. Staff should ensure that no part of the footage can be seen through

a window in a door or a window looking into the office from an external area. The office door should be completely closed for the duration of the viewing and for any discussions about the footage that may follow.

5.2 CCTV footage should be kept for a maximum of 30 days, unless an incident has occurred on School premises and the footage is to be kept for a purpose. CCTV footage is stored securely in a lockable office / on the School's password protected software system. If an incident has occurred, the footage in question should be stored in a secure environment, pending further action. Once the action/investigation has been concluded, a review of the retention of the footage should be exercised and secure disposal of the footage should occur where it is no longer needed for a valid purpose.

5.3 The School has developed a form called the "CCTV Disclosure Record" and it must be completed on every occasion that footage is viewed or disclosed to a third party. The form should be forwarded to the Data Protection Officer as and when a valid request for CCTV footage is made. The form can be located on the School's internal shared drive. The record will include the following:

5.3.1 the purpose of any searches and whether the search was successful or not.
5.3.2 who carried out the search
5.3.3 persons present (particularly when reviewing).
5.3.4 date, start and end time of the incident.
5.3.5 date and time of the review
5.3.6 any other relevant information

6. DISCLOSURE OF IMAGES

6.1 The School will ensure that any disclosure of images is in a controlled manner and that the disclosure is consistent with their data mapping and privacy notice in regards to CCTV.

6.2 There will be no disclosure of recorded data to third parties unless permission is obtained from the appropriate person following their consultation with the School's DPO. It is acceptable for the School to disclose images to law enforcement agencies for the purpose of prevention and detection of crime. These requests should be in writing wherever possible and the disclosure should be clearly documented by the School as outlined in clause 5.3.

6.3 The school will document in their DPIA how personal information will be shared. In the case of a disclosure request from law enforcement or a valid subject access request, the recording pertaining to the request will be downloaded onto a portable device and securely stored in a locked room until collection. The file will be encrypted or password protected where possible. Alternatively, the recording will be sent in a password protected document via email. Staff will ensure passwords are sent separately from the email containing the recording, ensuring that the original copy of the recording is kept at the School.

6.4 If the immediate viewing of a document is necessary, this will be governed by clause 5 above.

6.5 In cases where disclosure is requested by a third party who does not appear on the footage, extreme caution should be taken and the DPO referred to. Where this is a parent on behalf of a pupil, the Subject Access Guidance should be followed.

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

7. AUTHORISED PERSONNEL AND CIRCUMSTANCES

7.1 Authorised Personnel at Gosford Park Primary School are: Headteacher, Deputy Headteacher, School Business Manager and Office staff. Training is being provided to these staff, by the City Council's Data Protection Officer in handling both CCTV data and access requests. However, there may be occasions that will require contractors to view the monitors during the recording of live images and also images that have been recorded previously. It is important to remember that the viewing of all images from a CCTV system must be controlled and consistent with the purpose for which the system was installed. On a routine basis, this means that teaching and support staff cannot request to access footage.

7.2 Appropriate personnel will allow third parties to view live and recorded images for maintenance purposes and in compliance with the objectives of the CCTV objectives set out in paragraph 4.

7.3 The School's DPO may be involved in any circumstances where the School feels advice is necessary. Where the School is unsure of whether to seek advice from the DPO, for the avoidance of doubt advice should be sought.

8. USE OF AUDIO RECORDING WITH CCTV

8.1 The use of CCTV recording involving audio recording between members of the public is highly intrusive and unlikely to be justified. The CCTV system has the facility for audio however it will only be accessed whilst reviewing footage as outlined in 5.1.

9. BREACHES

9.1 A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

9.2 Any breach of security will be initially investigated by the School's appropriate personnel, in order to discuss this further with the School's DPO, governing body and Senior Leadership Team. The School's DPO may initiate communications to the ICO, within the 72 hour period, in cases where the breach could lead to or has led to a risk of harm. The School's DPO may extend the communications to those affected by the breach, in order to provide them with the details in regards to the breach of their personal information and how they can take precautions from further consequences of the breach.

9.3 The School may take the appropriate disciplinary action in the relevant circumstances. A breach of this policy will be governed by the School's code of conduct and disciplinary procedure. Any serious breach of the CCTV Policy[1] may be concluded to be a form of gross misconduct. It will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach. This investigation will involve the input of the School's DPO.

9.4 A breach of security in relation to CCTV footage will be actioned in line with the School's Breach Procedure.

Where a criminal offence has been committed on School premises, the School is not under any duty to release the footage to or allow it to be viewed by the subject, their family or friends. Any unauthorised disclosure of the footage may prejudice any subsequent police enquiry. The footage should be downloaded onto disk/memory stick/email attachments and given directly to the police as evidence, following the production by the police of a valid request for disclosure. When an incident occurs on School premises during evenings and weekends, it would be necessary to contact the Site Services Manager or appropriate person. This means that on those occasions the Site Services Manager or appropriate person would be an authorised person in order to view footage and in an emergency, disclose it to the police. On receipt of a 'routine' subject access request by an individual, the Site Services Manager or appropriate person should ask the requestor to complete a 'Subject Access Request' form available on the School's website and send it to the School's email address.
If the Site Services Manager or appropriate person receives a request from the police, but it is not an emergency, the request should be directed to the School's email address to be dealt with during normal office hours.

10. CCTV and GDPR

10.1 In order to comply with the right to be informed, significant signage is found in prominent positions in all areas where CCTV cameras operate to inform staff, students and the general public that they are entering an area where their images are being recorded either as still or video footage. Employee, parent, pupil and visitor privacy notices include the information that the school uses CCTV cameras.

10.2 The right for individuals to request access to their data can be exercised using a subject access request template on the school's website.

10.3 The right to object/restrict processing may be possible in certain circumstances. However, this will be considered on a case by case basis.

10.4 The right to rectification will apply where possible.

10.5 The right to data portability is not applicable as CCTV is filmed under the public task duty. Automated decision making is not included in this process.

10.6 Data minimisation is exercised with the automated deletion of CCTV footage after 30 days, unless an exemption to the rule applies. For example a police investigation is ongoing.

10.7 The right to erasure is considered where the personal data is no longer necessary in relation to the purposes for which it was processed.

10.8 All rights can be exercised by individuals contacting the School or the named DPO.

11. SUBJECT ACCESS REQUESTS

11.1 Individuals have the right to request access to CCTV footage relating to themselves under the GDPR and DPA. The Subject Access Guidance will be followed.

11.2 All requests should be made in writing to the School. 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.

11.3 The School will respond to a request within one calendar month of receiving a valid request.

11.4 Where a subject access request includes footage of another individual not included in the request, the school must either use 'blurring' to distort the images to only the relevant individual, or gain consent to disclose third party personal data from those individuals not involved in the request.

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

11.6 The School will notify the requester if an exemption or limitation to their request applies, such as:

11.7.1 A claim to legal professional privilege in legal proceedings

11.7.2 The request will infringe on a third party's rights and freedoms
11.7.3 Any other exemption to the right of access as stated in the GDPR and DPA.

12. APPEALS

12.1 There is a School 'Subject Access Procedure' that should be followed in the event that an individual is refused access to CCTV images and they are not satisfied with this outcome or the reasons why access has been refused. The appeal procedure will be provided upon an acknowledgement response from the School to the individual making the Subject Access Request.

13. COMPLAINTS

13.1 Complaints and enquiries about the operation of CCTV within the school should be addressed through the School's complaints procedure. Where necessary, the School's Data Protection Officer will be informed of the complaint.

I have read and understood the terms of this Policy. I understand that I must adhere to this Policy at all times.