PARK SCHOOL AND LITTLE CRICKETS
AT PARK SCHOOL

VISITORS, SECURITY AND CCTV POLICY

Applicable to the whole school, including the Early Years Foundation Stage (EYFS) and Little Crickets at Park School

Policy reference	Visitors, Security and CCTV Policy
Policy owner	Headteacher / Designated Safeguarding Lead / Data Protection Officer
Approved by	School leadership / proprietor
Review cycle	Annually and sooner following material legal, regulatory or operational change
Next review	Summer 2027
Related documents	Safeguarding and Child Protection Policy; Data Protection Policy and Privacy Notices; Emergency and Fire Procedures; Safer Recruitment Policy; Behaviour Policy; Health and Safety Policy

1. Purpose and scope

This policy sets out the arrangements used by Park School and Little Crickets at Park School (together, "the School") to control access to the site, manage visitors and contractors, maintain physical security, and operate closed-circuit television (CCTV) lawfully and proportionately.

It applies to pupils, children in the EYFS, staff, agency workers, volunteers, governors or proprietors, contractors, visitors, parents and carers, and members of the public while on School premises or when their personal data is captured by the School's CCTV system.

Safeguarding is everyone's responsibility. Any concern about a child, an adult's conduct, site security or unauthorised access must be reported immediately through the School's safeguarding and emergency procedures.

2. Legal and guidance framework

The School will have regard to the following, as applicable:

- Keeping Children Safe in Education 2026 and the School's Safeguarding and Child Protection Policy;
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018;
- Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice, where applicable;
- Information Commissioner's Office guidance on video surveillance, data protection principles, access requests and data security;
- Equality Act 2010, including the duty to make reasonable adjustments;
- Early Years Foundation Stage statutory framework requirements relating to safeguarding and the security of premises; and
- Health and Safety at Work etc. Act 1974 and associated health and safety duties.

This policy must be read alongside the related documents listed in the policy information table. Where there is any conflict, current legislation and statutory guidance take precedence.

3. Roles and responsibilities

The Headteacher has overall responsibility for ensuring that suitable visitor, security and CCTV arrangements are implemented and reviewed.

The Designated Safeguarding Lead (DSL) oversees safeguarding arrangements for visitors, visiting speakers and concerns arising from a visit or CCTV footage.

The Data Protection Officer (DPO) advises on data protection compliance, privacy information, data protection impact assessments, access requests, complaints and data breaches involving CCTV.

The Site Manager is responsible for day-to-day site security and acts as CCTV System Manager unless another suitable person is formally appointed. Responsibilities include opening and securing the site, routine security checks, camera checks, access controls and maintaining relevant logs.

All staff must follow sign-in and sign-out arrangements, wear identification, challenge unidentified adults appropriately, supervise visitors where required, and report concerns without delay.

4. Site security and access control

- The Site Manager, or an authorised deputy, will unlock the premises and secure them at the end of the day. Staff must close windows and doors, switch off equipment as required and report defects.
- Pupils enter from 8.30 am and external gates are secured at 8.45 am. Entry after this time is controlled through the School Office. Little Crickets arrangements must remain consistent with the setting's authorised collection and safeguarding procedures.
- Doors, windows, gates, fencing, locks, lighting, alarms and pedestrian routes will be maintained in good order. Hazards will be isolated or clearly marked and reported for prompt action.
- Key, fob and access-code holders will be authorised, recorded and reviewed. Keys and access credentials must not be shared with unauthorised persons. Emergency contact arrangements will be held securely and shared only where necessary.
- Any loss of keys, fobs, identification badges or suspected compromise of an access code must be reported immediately to the School Office and Site Manager.
- Adults on site must sign in as required and display the correct School-issued identification, badge or lanyard. Anyone without visible identification should be politely challenged and directed to the School Office.
- Personal security information, including access codes and CCTV login details, must not be displayed, discussed publicly or included in general communications.

5. Staff identification and movement on site

- Staff must wear their School staff lanyard and photo identification clearly while on the premises. The safeguarding team may use its designated identifying lanyard.
- Staff must sign in and out electronically using the School's approved system, including when leaving and returning during the working day.
- Staff must not permit another person to tailgate through a secure entrance. Doors and gates must not be wedged open unless this is part of an authorised and supervised arrangement.
- Staff must immediately report suspicious behaviour, unauthorised access, damaged security equipment or any situation that may place children or adults at risk.

6. Visitor procedures

All visitors must report to the School Office unless a specific, risk-assessed arrangement has been authorised for an event. The following minimum procedure applies:

1. The visitor provides their name, organisation, host and purpose of visit and, where required, suitable photographic identification.
2. The visitor signs in electronically and confirms that they have read or received the relevant safeguarding, emergency, evacuation, confidentiality and conduct information.
3. The visitor is issued with a dated photo badge or appropriate lanyard and wears it visibly throughout the visit.
4. The host collects the visitor from the School Office, remains responsible for the visitor and ensures the required level of supervision.
5. The visitor signs out, returns any pass or lanyard and is escorted from the site where appropriate.

Visitors must not take photographs, video or audio recordings, access pupil information, use unauthorised devices, or enter restricted areas unless expressly authorised. Personal devices must be used in accordance with School policy.

Parents and carers attending routine drop-off, collection, performances or public events will follow the access arrangements communicated for that activity. Attendance at an event does not permit unsupervised access to other parts of the premises.

7. Visiting speakers and visitors working with children

- The inviting member of staff must complete the School's internal visitor or visiting speaker approval process in advance and submit it to the DSL.
- The School will make proportionate checks on identity, suitability, credentials, the proposed content and safeguarding risk. Checks must be recorded by the DSL or authorised person.
- Content must be age-appropriate, consistent with the School's ethos and legal duties, and must not undermine fundamental British values or expose children to harmful or inappropriate material.
- Unless the School has confirmed that the visitor may work unsupervised and all required checks are in place, the visitor must remain under direct staff supervision and must not be left alone with children.
- Any safeguarding concern arising before, during or after the visit must be reported immediately to the DSL and managed under the Safeguarding and Child Protection Policy.

8. Contractors and agency personnel

- Contractors must sign in, provide suitable identification and wear the designated contractor or visitor pass.
- The School will determine the appropriate checks and supervision by considering the nature, location, duration and timing of the work and the opportunity for contact with children.
- A contractor whose required DBS or other suitability checks have not been verified must not have unsupervised access to children and must be supervised in accordance with the School's risk assessment.
- Contractors must receive relevant safeguarding, fire, emergency, first-aid, asbestos and site safety information before work begins, as applicable.
- For significant work, contractors must provide suitable risk assessments, method statements and evidence of competence and insurance where required.
- Work areas, tools, substances and access routes must be secured. Work likely to create additional risk should, where practicable, be scheduled away from children.

9. Accessibility and reasonable adjustments

Visitors with disabilities or additional access needs will be treated with dignity and supported through appropriate reasonable adjustments. The host should establish relevant needs in advance where practicable, agree a safe access and evacuation plan, and arrange assistance without making assumptions about the person's abilities.

Where a route or area presents an access difficulty, the School will consider a suitable alternative. The wheelchair ramp is available by the hall entrance; staff must ensure it is used safely and does not obstruct an escape route.

10. Unidentified, unauthorised or threatening persons

- Staff should use calm, non-confrontational language, maintain personal safety and ask the person to accompany them to the School Office.
- If the person refuses, behaves suspiciously, becomes threatening or attempts to access children or restricted areas, staff must contact the School Office, Site Manager or Senior Leadership Team immediately using the School's agreed alert procedure.
- Children must be moved away from risk. Staff must not place themselves in danger or attempt physical intervention unless this is necessary, lawful and consistent with School policy.
- The Headteacher or senior leader will decide whether to initiate lockdown or other emergency arrangements and whether to call the police. In an immediate emergency, call 999.
- The incident must be recorded and any safeguarding, health and safety, data protection or premises follow-up completed.

11. Emergency and evacuation arrangements

Hosts are responsible for ensuring visitors understand relevant emergency procedures and are accounted for during an evacuation or lockdown. For public events, the organiser must provide suitable safety information at the start or through clear written or displayed instructions. The electronic or manual visitor register must be available to the person coordinating the emergency response.

CCTV ARRANGEMENTS

12. Purpose and lawful use of CCTV

The School is the Data Controller for its CCTV system. CCTV is used only where necessary and proportionate for defined purposes, including:

- protecting pupils, children, staff, volunteers, visitors and members of the public;
- protecting buildings, equipment and personal property;
- preventing and detecting crime and assisting lawful investigations;
- monitoring the security and integrity of the site, entrances, exits, deliveries, arrivals and relevant parking areas;
- establishing relevant facts in safeguarding, health and safety or serious behaviour incidents; and
- monitoring contractors or work activity where this is necessary for security or safety.

CCTV will not be used for routine staff performance monitoring. It may be reviewed in relation to a specific incident where this is necessary, lawful and proportionate. Images will not be used for commercial purposes.

The School relies on an appropriate lawful basis under data protection law and records its assessment in its data protection documentation. The School maintains a Data Protection Impact Assessment (DPIA) for CCTV and reviews it when the system, purpose, coverage or risk materially changes.

13. Camera positioning and transparency

- Fixed cameras are visible and are generally positioned externally to monitor entrances, exits and limited playground or boundary areas.
- No camera will be positioned to capture areas where individuals have a heightened expectation of privacy, including toilets, washrooms, changing rooms or medical rooms.
- Public areas and neighbouring property will not be captured except where unavoidable and limited at site entrances. Camera angles and privacy settings will be adjusted to minimise unnecessary recording.
- Prominent signs will identify that CCTV is in operation, state the School's identity as Data Controller, explain the main purpose and provide a contact point for further information.
- Covert surveillance will not be undertaken routinely. Any exceptional proposal must be lawful, strictly necessary, time-limited, authorised at the appropriate level and supported by specific DPO advice and a DPIA.

14. Operation, maintenance and security of the system

- The CCTV system operates continuously, subject to equipment availability, maintenance and power or network interruption.
- The System Manager will check recording and camera functionality regularly and arrange servicing at least annually or sooner where a fault is identified.
- Access accounts must be individual where the system permits, protected by strong credentials and limited to authorised roles. Access must be removed promptly when no longer required.
- Live and recorded images must be viewed only in a suitably secure and private location. Screens must not be visible to unauthorised persons.
- CCTV equipment, storage devices, exported images and system logs must be protected against unauthorised access, alteration, loss or disclosure.
- Any suspected CCTV data breach must be reported immediately under the School's data breach procedure and escalated to the DPO.

15. Authorised access and supervision

Routine system supervision is limited to the Site Manager, Headteacher and School Business Manager, or other staff specifically authorised in writing. The System Manager must verify the identity and authority of anyone requesting access and must be satisfied that the request is legitimate, necessary and proportionate.

The DSL or an appointed deputy may view relevant footage where this is necessary to assess or respond to a safeguarding concern. Access by other staff is not permitted merely because they are involved in an incident.

16. Retention, preservation and deletion

Recorded images are normally retained for 30 days and then overwritten automatically. Footage may be preserved for longer where this is necessary for a safeguarding matter, complaint, insurance claim, disciplinary or behaviour process, legal claim, police request or other lawful purpose.

Preserved footage will be kept securely, access will be restricted, and it will be deleted when no longer required. The School will keep a disclosure or access log recording the date and time, requester, authoriser, reason, footage viewed or exported, outcome, retention decision and any relevant incident or crime reference.

17. Viewing and disclosure of images

CCTV images may be viewed or disclosed only where lawful and necessary. Examples include:

- a request from the Headteacher, DSL, police, court, local authority or another body with a lawful basis;
- investigation of suspected criminal conduct, safeguarding concerns, serious misconduct, unacceptable pupil behaviour, damage or an insurance claim;
- response to a valid data subject access request; or
- another circumstance required or permitted by law.

Before disclosure, the School will consider the rights of other identifiable people. Where practicable, non-relevant individuals will be obscured or the request will be addressed by another lawful method. Copies must be transferred securely and the disclosure recorded.

18. Individual rights and requests for footage

Individuals may have the right to request access to personal data about them captured by CCTV. Requests should be sent to the School and should include enough information to locate the footage, normally the date, approximate time, location or camera, and a description of the person concerned. Proof of identity may be required.

Requests will be handled under the School's Data Protection Policy and applicable timescales. Access may be restricted where an exemption applies or where disclosure would adversely affect the rights of others. Because footage is routinely overwritten after 30 days, a request should be made promptly; however, the School will not preserve or disclose footage unless there is a lawful basis to do so.

19. Third-party CCTV

The School does not control CCTV operated by third parties, such as transport providers, neighbouring premises or event venues. Where the School receives third-party footage, it will use and store it only where there is a lawful and proportionate reason consistent with safeguarding, behaviour, safety, security or legal obligations.

Where coach or transport CCTV is used to establish facts about an incident involving pupils, the matter will be managed under the relevant School policy and parents or carers will be informed where appropriate, subject to safeguarding and legal considerations.

20. Records, monitoring and review

The School will maintain appropriate records, which may include visitor registers, visiting speaker approvals, contractor checks, incident reports, key and access-control records, CCTV maintenance checks, the CCTV DPIA, authorisation records and viewing or disclosure logs.

The Headteacher, DSL, Site Manager and DPO will review the effectiveness of these arrangements as part of the School's safeguarding, premises and data protection oversight. Lessons from incidents, complaints, near misses, system changes and regulatory guidance will be incorporated promptly.

21. Complaints and queries

Operational or safeguarding concerns should be referred to the Headteacher or DSL. Questions about personal data, CCTV rights, access requests or privacy should be referred to the DPO. Complaints will be handled under the School's Complaints Policy and Data Protection Policy, as appropriate. Individuals may also raise a concern with the Information Commissioner's Office after giving the School an opportunity to respond.

22. Approval and policy history

Version	Date	Summary of change	Approved by
1.0	October 2026	Combined and updated Visitors and Security Policy and CCTV Policy; terminology, responsibilities, safeguarding, accessibility and data protection provisions aligned.	To be completed