Claregate Primary School - CCTV Policy

Date of Policy March 2022. Date of Policy Review March 2023.

This policy was updated with regard to "Amended Surveillance Camera Code of Practice" November 2021.

Day to Day Management and operation of CCTV

The use of CCTV is covered by the General Data Protection Regulations 2018.
The data protection controller is Mr M Murphy the Headteacher
The Data Protection Officer is Mrs K Elliott (Headteacher, Long Knowle, Primary School).

There are cameras located around the outdoors of the school, mainly onto playgrounds, entry and exits points. There are no CCTV or any recording devices in toilet areas. Pupils often mistake PIR movement sensors as part of an intruder alarm as cameras – they are not! Images are displayed on a screen in the Headteacher's office and in the general office and not in communal areas. There is no body worn footage recorded in school. Recording technology is in the Headteacher's office.
The Headteacher or Deputy Headteacher in his absence manage access to the images and control panel in the Headteacher's office. Recorded images can only be gained via a security password and are not used on a wireless system.
CCTV images of outdoor areas can also be monitored remotely via an app on mobile telephones. It is possible to view the school site from home in the event of a suspected burglary. This prevents unnecessary journeys in non-working hours and ensures that the correct emergency services can be contacted and given "confirmed" status of for example a break in. It also provides information for safer entry to the site if the Site Manager needs to re-set the alarm and helps to prevent going onto the site if potentially aggressive people are there.
CCTV images are not routinely backed up to a central or remote server, but images of significant incidents which need to be preserved beyond 10 weeks, may be stored on the server which is password protected and only available to the Headteacher and Deputy Headteacher.
CCTV is declared under notification procedures re Data Protection Act.
Cameras are situated in areas where monitoring is most required i.e. where theft or anti- social activity is most likely to take place.
CCTV signs letting people know it is being used are at the two points of entry to the school site at the front and back gate. Periodic reminders will be put on newsletters about the use and it is on the school prospectus.

There is one camera indoors in the "sensory room" where it is more likely for members of staff to be working in smaller groups and is displayed and recorded in the Inclusion Leader's office.
The main CCTV system is redacted so that areas outside of the school grounds cannot be seen or recorded by CCTV e.g. neighbours property.

The aims of using CCTV in school are :-

1. **Monitoring**

To watch the flow of pupil movement around the school and identify if there are any bottlenecks, potential Health and Safety issues, or people in areas of the school where it is inappropriate for them to be.

2. **Detecting**

To know that someone is present even if you cannot see their face.

3. **Recognising**

Helping to recognise people at the front door who are requesting access to the school. Potentially denying access to those who we recognise as risky people, or those whom the office staff or Headteacher do not want to enter the building.

4. **Identifying**

- Gaining images which may help to identify those committing a crime during, or out of school hours. Or indeed the way a crime was committed if individuals are not identifiable.
- Safeguard children and adults by providing a traceable image of those who may wish to harm children, or of incidents that are threatening.
- Providing footage to the police or child protection agencies of alleged criminal activity or safeguarding issues. These images could be used in a court of law.
- Providing recorded images to trace the build up to and alleged incidents.
- Matters of gross misconduct, risky behaviour or criminality on the part of staff i.e. matters that cannot be ignored.

CCTV is <u>not</u> for the purposes of :-

- Infringing an individual's human rights or their privacy
- To provide images to a third party for publishing e.g. a TV company or social media.
- To monitor private property, or any public area which is not part of the school.
- Recording conversations (there is no audio recording installed).
- Biometric analysis such as facial recognition technology or automatic recognition systems.
- Routinely monitoring the capability of staff.

In line with HRA 19987 not to infringe

- the right to respect for private and family life (Article 8);
- freedom of thought, conscience and religion (Article 9);
- freedom of expression (Article 10);
- freedom of assembly and association (Article 11); and
- protection from discrimination (Article 14).

DFE Surveillance and monitoring in residential childcare settings published 3 October 2019

This is not intended for the maintained Primary Sector, however we are using the principles of policy below.

As a minimum, your policy should set out:

- the legitimate purpose and aim of the surveillance, with each purpose and activity individually addressed

  This is detailed above.

- how the surveillance will keep children safe

  If children know that they can be seen remotely and their actions can be followed up, their behaviour is more likely to be safe to themselves and each other.

  It can identify the presence of intruders or provide evidence of wrongdoing of adults.

  It can help us to learn lessons from injuries or incidents.

It can provide evidence in the investigation of child safeguarding accusations or whistleblowing.

- why surveillance is the best way of achieving a child's safety

  We do not classify the use of CCTV strictly as surveillance, because it is not used to track an individual child. It is remote monitoring of a general area.

- how any data is processed and stored

  On a hard drive in the Headteacher's office and a separate one camera system in the "sensory room". It is occasionally transferred onto a CD or other hard drive if we wish to preserve an incident. Our CCTV is highly unlikely to be able to identify an individual beyond reasonable doubt in a court, as the image definition does not reach minimum standards.

- what security measures are in place to safeguard against unauthorised access and use

  There is a password to access recordings.

- how often the surveillance activity will be reviewed to ensure that it is still necessary

  When required to do so. We do not routinely sit and watch footage remotely, or monitor footage systematically at set times.

- how surveillance and monitoring activities are agreed with the placing authority, parents, carers and children (if appropriate)

  The policy is on the website and a sign on the gate telling people that CCTV is in operation. Children are told how we use CCTV in assemblies. Periodically we remind parents that CCTV operates through app messages and newsletters.

- how others (for example, health visitors) are notified that they are being recorded

  Notice on the gate and Staff Handbook.

Data Protection, Retention and Disclosure

There is no legal specific minimum or maximum time for footage to be stored. CCTV recordings are kept on our hard drive for 10 weeks and then automatically deleted. If data is passed onto other responsible agency e.g. the police, it will be put onto a disk for removal from site unless specifically requested to be by other means and then only if secure. If requested and GDPR rules allow, the data may be emailed by and to a secure email address It is then the responsibility of the other agency to safeguard their copy of the data provided under the GDPR.

Data breaches are reported to the Governing Board and ICR where necessary.

The school may disclose information and images to the Information Commissioner or the Investigatory Powers Tribunal.

Disclosure is a matter of discretion. Where a written request for disclosure is made e.g. a "subject access request" the data controller will decide to grant or refuse any request for disclosure, based on our Freedom of Information Policy and GDPR Policy. Where it is a matter of criminality or child protection / safeguarding and abuse or neglect is accused, it is highly likely that recordings will be disclosed to the police or child protection agencies. Where an individual is asking for copies of images of themselves or their child only, there is little reason to refuse.

However, being alone in a primary school is a rare occurrence and giving copies of recordings to parents, staff or some outside agencies may be refused, as it may infringe the privacy rights of children and adults who are also part of that recording.

It is unlikely to infringe privacy if there are innocuous occurrences e.g. people going about their daily business. Where it is a matter of factual accuracy, the data manager may decide to show a recording of an incident to a pupil or parent, without giving a copy. It is likely that this is to prove something their child has or has not done. Where sensitive data of another person may be disclosed by doing this, the school will seek express permission from that person / those with responsibility for that person and they have the right to refuse.

However, it is likely to invade privacy if there is a controversial incident. It is unlikely that we will show footage to prove what somebody else's child has done to their child as this may be a breach of privacy. In these circumstances, the data controller will watch and report factually on what has been seen. If this view of events is disputed, a second opinion from a member of school staff can be sought. If it is still disputed after that the school complaint policy should be followed.

Showing CCTV recording or images to children is not expected to be commonplace, but where it helps to clear up matters of factual accuracy in disputes of right or wrong it can be used selectively at the discretion of the data manager which is the Headteacher. These factual investigations have proved exceptionally helpful in establishing fact from speculative claims in the past.

Where a person insists on an image of themselves being disclosed, the school may ask for an external agency to, if possible, make a copy where other people are anonymised, or not shown on the recording. The full cost of this will be passed on to the person requesting this.

Where the school is unsure about whether it is disclosable or not, the data manager will seek legal advice from the local authority.

Complaints or Concerns

Complaints should follow the school complaint policy. This has an appropriate appeal system. Concerns can be voiced in person or via email communication. We will publish statistics about the number and nature of complaints received if there are any. Where a criminal offence may have taken place in relation to a surveillance camera system this will be reported to the police, ICO and the teacher Regulation Agency.

We define the following roles :-

- "System Operator" – person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.

  System operators are the Governing Board and they consider the balance between child and public protection and individual human rights. The system operator can refuse to disclose information held on CCTV.
- "System User" – person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such system.

  System users are the Headteacher and Deputy Headteacher. They decide why and how data is used proportionately, in line with the principles of this policy.
- "Commissioner" is the role undertaken by the Surveillance Camera Commissioner, as set out in Protection of Freedoms Act 2012. To encourage compliance with this code, it is the function of the Commissioner to provide information and advice on all matters within this code relevant to surveillance camera systems.