Chilwell *School*

Queens Road West, Chilwell, Nottingham NG9 5AL

T: 0115 925 2698 E: office@chilwellschool.co.uk
F: 0115 925 8167 W: www.chilwellschool.co.uk

Head Teacher: Sarah Baxter-Williams

CCTV and Surveillance Policy

1. Introduction

1.1. Chilwell School is committed to safeguarding and the welfare of our pupils/students, staff, and visitors. This policy sets out the management, operation and use of CCTV surveillance systems in our school.

1.2. We use CCTV and Surveillance systems to:

- protect School buildings, grounds and assets.
- increase personal safety and reduce the fear of crime.
- support the police in deterring and detecting crime.
- assist in managing the School.

1.3. The systems will not be used:

- to provide recorded images for the world-wide-web.
- to record sound.
- for any automated decision taking.

1.4. This policy will be reviewed annually.

2. Definitions

2.1. "Data Controller" means the School's Data Controller

2.2. "Surveillance systems" includes CCTV systems and access control systems.

2.3. "Surveillance staff" means employees of the School, which may include senior leadership or administrators or premises staff, with the skills and permission to manage and operate surveillance systems.

3. Statement of Intent

3.1. Surveillance systems are registered with the Information Commissioner under the terms of the Data Protection Act 2018. Chilwell school will comply with the requirements of both

the Data Protection Act and the Commissioner's CCTV Code of Practice. The school will treat all surveillance schemes and all information, documents and recordings obtained and used as data which are protected by the Act.

3.2. Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by School CCTV.
3.3. Materials or knowledge secured as a result of CCTV or access control systems will not be used for any commercial purpose. Data will only be released for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

3.4. Systems are planned and designed to give maximum effectiveness, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. CCTV systems may include fixed or mobile cameras located around the school site.

3.5. Cameras will not focus on private homes, gardens and other areas of private property. Cameras will be positioned where possible to avoid capturing the images of persons not visiting the premises.

3.6. CCTV systems which make use of wireless communication links (eg, transmitting images between cameras and a receiver) should ensure that these signals are encrypted to prevent interception.

3.7. CCTV systems which can transmit images over the internet (eg, to allow viewing from a remote location) should ensure that these signals are encrypted to prevent interception and also require some form of authentication for access (eg, a username and secure password).

3.8. Schools must ensure that cameras and systems produce clear images which law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.

4. Management of Surveillance systems

4.1. Surveillance systems will be administered and managed by the IT Team, in accordance with the principles and objectives expressed in the code. The IT Team are responsible for undertaking systematic checks of the management, operation and retention of data under this policy and recording such checks on the Surveillance Log. In the event of external requests from crime prevention bodies a written request to the Head Teacher is required.

4.2. Surveillance systems will be operated 24 hours each day, every day of the year.

4.3. Surveillance system controls and hardware will only be accessed by Surveillance staff or authorised personnel. Full details of access must be recorded in the School's Surveillance log.

4.4. Day-to-day management is the responsibility of designated Surveillance staff. Surveillance staff will:

- check and confirm the efficiency of the system regularly including checking that cameras are functional and not obscured, recording and overwrite functions are as designed
- ensure appropriate technical, physical and organisational security of systems
- ensure system maintenance is up to date

4.5. CCTV footage will only be retained for a maximum of 14 days. This means the right of erasure may not apply as erasure will happen automatically after 14 days. On occasion, we may need to retain data for a longer period, for example, where a law enforcement body is investigating a crime and asks for it to be preserved, to give them the opportunity to view the information as part of an active investigation or where the school is investigating an incident. After this time, we will permanently delete the data through secure methods.

5. Data sharing

5.1. Release of data to the police or other authorised applicants will be upon written request to the Head Teacher.

5.2. Requests by the police can only be actioned under section 29 of the Data Protection Act 1998. Recordings will only be released to the police on the clear understanding that the recording remains the property of the School, and both the recording and information contained on it are to be treated in accordance with this code. The School also retains the right to refuse permission for the police to pass to any other person the recording or any part of the information contained thereon.

5.3. Applications received from outside bodies (for example solicitors) to view or release recordings will be referred to the Head teacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a court order.

5.4. The Data Protection Act provides data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV. Requests for data subject access can be made in accordance with the school's Subject Access

Request Policy and must include the date, time and location where the footage is believed to have been captured. Where information of third parties is also shown with the information of the person who has made the access request, we will consider whether we are able to release this information.

5.5. Requests under the Freedom of Information Act will be considered following the guidance in the ICO's CCTV Code of Practice in conjunction with safeguarding laws.

6. Breaches

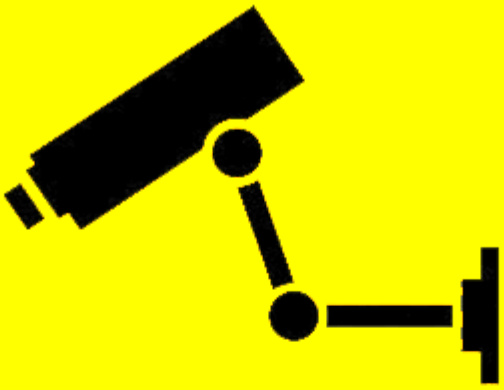
6.1. Any breach of this policy will be investigated by the Headteacher and the school's Data Protection Officer in line with the school's Personal Data Breach Policy.

7. Complaints

7.1. Any complaints about the School's Surveillance systems can be made via the school's Complaints Policy.

8. Appendices

1. CCTV Signage (print on yellow paper) or ensure similar signage is displayed
2. CCTV Footage Request Log



CCTV

Images are being monitored for the purpose of public safety, crime prevention, detection and the prosecution of offenders.

This scheme is controlled by

Chilwell School

For further information please visit

http://www.chilwellschool.co.uk

Google Form - CCTV Footage Request Log

- Name of person requesting CCTV footage
- Position
- Location of camera
- Date of incident
- Start time
- End time
- Why do you need the footage?