GILBERT INGLEFIELD ACADEMY

CCTV POLICY

Date of Policy:	October 2024
Approved by Chair of Governors:	October 2024
Next Review Date	October 2027
Staff Responsible:	Data Protection Lead Data Protection Officer IT Department

1. Policy statement and objectives

1.1 Gilbert Inglefield Academy (the School) has a CCTV surveillance system in place on its site. The purpose of this policy is to set out the responsibilities of the School regarding the management, operation and use of the CCTV system, and details the procedures to be followed in order to ensure that the School complies with relevant legislation.

1.2 This policy applies to all members of our staff, visitors to the site and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2. Purpose of the CCTV system

2.1 The principal purposes of the CCTV system are as follows:

- to ensure the safety of staff, students and visitors;
- for the prevention, reduction, detection and investigation of crime and other incidents;
- to assist in the investigation of suspected breaches of School rules

2.2 The School intends to use CCTV for the purposes of:

- providing a safe and secure environment for students, staff and visitors;
- protecting the School buildings and assets, both during and after hours;
- reducing the incidence of vandalism, bullying, anti-social behaviour and site incursion
- enabling a faster and more effective resolution to incidents by assisting staff in identifying persons who have committed a breach of the School rules;
- safeguarding students absent from lessons through visible checks about location during the school day and during lunch;
- assisting in the prevention of crime and assisting law enforcement agencies in apprehending offenders

2.3 The use of the CCTV system will be conducted in a professional, ethical and legal manner and only for the intended purposes. Any member of staff who misuses the CCTV system may be committing a criminal offence and will face disciplinary action.

3. Overview of the CCTV System

3.1 The CCTV system is owned and managed by the School. Under current data protection legislation, the School is the 'data controller' for the images produced by the CCTV system. Recognisable images captured by CCTV systems are 'personal data'.

3.2 The CCTV system operates to meet the requirements of the current data protection legislation and the ICO's guidance.

3.3 The CCTV system produces clear images which are suitable for the intended purposes, and which can easily be taken from the system when required.

3.4 The system comprises of over 60 fixed cameras. The School has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.

3.5 Cameras are sited to ensure that they only capture images relevant to the purposes for which they are installed.

3.6 Cameras placed to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property. Care will be taken to ensure that reasonable privacy expectations are not violated.

3.7 CCTV may be used in classrooms and teaching areas if deemed necessary by senior leadership and only after the agreement of affected teaching and support staff has been obtained.

3.8 CCTV systems may be used to monitor normal teacher/student classroom activity if deemed necessary by senior leadership and only after the agreement of affected teaching and support staff has been obtained.

3.9 CCTV warning signs are clearly and prominently placed at all external entrances to the site and around the site to indicate that CCTV is in operation, how long images are stored, and contact details in the event of a query about the CCTV system.

4. Monitoring and Recording

4.1 The viewing of live CCTV images and recorded images which are stored by the CCTV system will be restricted to authorised staff.

4.2 "Authorised staff" means data protection lead, IT department staff, senior leadership team, key stage and deputy key stage leads and behaviour leads.

4.3 All authorised staff are aware of the procedures that need to be followed when accessing the recorded images. All staff are aware of the restrictions in relation to access to, and disclosure of, recorded images.

4.4 Relevant images may be shared with governing body panels reviewing exclusions, disciplinary matters or complaints.

4.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to the disclosure of images.

4.6 Monitoring and recording of public areas may include the following:

- the building's perimeter, main entrance/exit gates, lobbies and corridors, restricted access areas at entrances to buildings and other areas;
- door controls, external alarms;
- parking areas, adjacent public highway

5. Storage and Retention of Images

5.1 The images captured by the CCTV system will be retained for a maximum of 30 days from the date of recording, except where the image identifies an issue and is required to be retained specifically in the context of an investigation/prosecution of that issue.

5.2 Clips of such retained recorded images are stored in a secure area accessed only by authorised staff. The storage of the clips is curated regularly, and clips will be deleted after 90 days unless a member of authorised staff informs the IT department that the clip is still required to be retained specifically in the context of an investigation/prosecution of that issue.

6. Disclosure of Images

6.1 Requests by individual data subjects for images relating to themselves will be treated as a 'Subject Access Request' and should be submitted in writing to the data protection lead Samantha Sibley dpo@gilbertinglefield.com together with proof of identification. Further details of this process can be found in our Subject Access Request policy, available on our website www.gilbertinglefield.com.

6.2 To locate the images, sufficient detail must be provided by the data subject to allow the relevant images to be located.

6.3 Where the School is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

6.4 The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the data protection legislation. In some circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation. Relevant images may also be shared with governing body panels reviewing exclusions, disciplinary matters, or complaints.

6.5 All such disclosures will be made at the discretion of the data protection lead and the data protection officer (DPO).

6.6 A record of any disclosure made under this policy will be held on the CCTV management system, detailing the date, time, camera, requestor, authoriser, and reason for the disclosure.

7. Data Protection Impact Assessment

7.1 Prior to the installation or repositioning of any CCTV camera, or system, a data protection impact assessment (DPIA) is required to be conducted by the School to ensure that the proposed installation is compliant with legislation and ICO guidance. The assessment will be approved by the data protection lead.

7.2 The School will adopt a privacy by design approach when installing new cameras and systems, considering the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

8. Complaints Procedures

8.1 Complaints concerning the School's use of its CCTV system or the disclosure of CCTV images should be made in writing to our data protection lead Samantha Sibley dpo@gilbertinglefield.com.

9. Policy and CCTV System Review

9.1 This policy is reviewed every three years with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

9.2 The School carries out an internal assessment annually to evaluate the usage and effectiveness of the CCTV system.