

CCTV Policy



Head of Tuition Service: Ruth Minhall

Head of Maypole Farm: Jamie Pickles

Approved: 01 October 2024

Signed: Ruth Minhall

Position: CEO

Last reviewed: Sept 2026

Next review: Sept 2027

Contents

Contents	0
1. CCTV STANDARD AND THE LAW	1
2. WHY THE SERVICE USES CCTV	2
3. HOW THE SERVICE USES CCTV	3
4. OBJECTIVES OF THE CCTV SYSTEM	5
5. STORING AND VIEWING IMAGES	5
6. DISCLOSURE OF IMAGES	7
7. AUTHORISED PERSONNEL AND CIRCUMSTANCES	7
8. BREACHES	8
9. CCTV and GDPR	9
10. SUBJECT ACCESS REQUESTS	10
11 FREEDOM OF INFORMATION	11
12 APPEALS	12
13 COMPLAINTS	12
14 REVIEW	12
School / Education Service CCTV SYSTEM ACCESS LOG	13
SECTION A: Requester & Authorisation Details	13
SECTION B: Purpose of Access	14
SECTION C: Footage Details & Action Taken	15
SECTION D: Data Protection Compliance Declaration	16
Form Management Notes for the Administrator (Do not print on circulated form)	16

1. CCTV STANDARD AND THE LAW

- 1.1** Closed Circuit Television 'CCTV' and its use is governed by the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR), each as amended by the Data (Use and Access) Act 2025 (DUAA). The Service have a legal duty to comply with the relevant Data Protection Legislation. In operating CCTV the Service also has regard to the Information Commissioner's Office (ICO) guidance *Video surveillance (including guidance for organisations using CCTV)*, and to Department for Education guidance on data protection in schools. The Service is not a "relevant authority" for the purposes of the Protection of Freedoms Act 2012 and is therefore not bound by the Home Secretary's Surveillance Camera Code of Practice; the Service nonetheless treats the principles of that Code as a benchmark of good practice. This Policy is to ensure CCTV within the Service is controlled appropriately to facilitate the Service's legal obligations, best practice and to reduce risk of information loss. The CCTV Policy should be read in conjunction with the Service's additional policies.
- 1.2** The Service 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 Service is the data controller and is legally responsible for compliance with the GDPR and DPA. This Policy is not intended to replace procedures already in place within the Service that relate to the physical operation and use of the system.
- 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 Service'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 service.
- 1.4** CCTV can record personal data and sound 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 a lawful basis 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 Service 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 video surveillance guidance. All authorised employees are aware of the restrictions in relation to access to, and disclosure of, recorded images within this CCTV Policy. The CCTV Policy must be read by any person/employee/contractor who will process personal data belonging to the Controller, the Service. The Service will make this CCTV Policy a public facing document.

2. WHY THE SERVICE USES CCTV

- 1.1** The Service uses CCTV for the purpose of its legitimate interests, 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 Service can monitor occurrences on site and also the security of the buildings and grounds. The Service 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.
- 1.2 Lawful basis.** Tuition Extra (Kent) Ltd is a private company and is not a public authority. The Service does not therefore rely on the “public task” basis at Article 6(1)(e) of the UK GDPR. The Service relies on its legitimate interests under Article 6(1)(f) – namely the safety and safeguarding of pupils, staff and visitors, the security of its premises and assets, and the prevention and detection of crime. A written Legitimate Interests Assessment (LIA) is maintained, reviewed by the DPO and refreshed whenever the system or its purposes materially change. Where CCTV is used to meet a specific statutory duty, the Service may additionally rely on Article 6(1)(c) (legal obligation), and in an emergency on Article 6(1)(d) (vital interests).
- 1.3 Special category and criminal offence data.** CCTV footage may reveal special category personal data (for example a person’s ethnic origin, disability or health). Where the Service processes such data it additionally relies on Article 9(2)(g) of the UK GDPR (substantial public interest), together with the safeguarding of children and of individuals at risk condition in Schedule 1 of the Data Protection Act 2018. Where footage constitutes criminal offence data, the Service relies on the corresponding Schedule 1 condition. The Service maintains an Appropriate Policy Document, as required by the Data Protection Act 2018, setting out how it complies with the data protection principles and its retention and erasure policies for this data. The Appropriate Policy Document is reviewed by the DPO at least annually.
- 1.4 Children and vulnerable data subjects.** The Service provides tuition to children and young people, the majority of whom have Special Educational Needs and Disabilities (SEND). In assessing necessity and proportionality, and in applying the Data (Use and Access) Act 2025 requirement to take account of children’s higher protection matters, the Service gives specific weight to the fact that its data subjects are children who may be less able to understand or object to surveillance. Transparency material is produced in clear, age-appropriate and accessible formats.
- 1.5 What CCTV will not be used for.** The CCTV system will not be used to monitor individuals in places where they have a heightened expectation of privacy (including toilets, changing areas, medical or therapy rooms and staff rest areas); to follow or track particular individuals, other than during a live emergency incident; for the routine performance management of staff; for any commercial purpose; or for any purpose other than the objectives set out in section 4 of this Policy.
- 1.6 Emerging surveillance technologies.** The Service does not operate facial recognition technology, automatic number plate recognition, body worn video, drones or smart doorbell cameras, and does not use artificial intelligence to analyse, classify or score

CCTV footage. No such technology may be introduced without a completed Data Protection Impact Assessment, the advice of the DPO, safeguarding sign-off, and the prior approval of the CEO. Any proposal of this kind is also subject to the Service's AI Governance Framework.

3. HOW THE SERVICE 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 Service'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 cameras will not process data that may be deemed as 'excessive', such as capturing public areas outside the scope of the Service, 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 Service's management of premises will identify the most appropriate housing for the monitors, ensuring security and privacy. In maintained services 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, British Standards and consideration of the advice taken from the Service's DPO. This would need to take into account capturing the best view of buildings for the purposes of security and high risk areas around the Service. The cameras must be of such quality to satisfy the purposes of installing the CCTV.
 - C. The CCTV system is owned and operated by the service, and its deployment is determined by the Service's management team. Installation should be carried by an industry-approved installer. The Service's authorised personnel is responsible for ensuring that the cameras are working correctly and consistently and will be responsible for ensuring they are maintained. This may mean retaining the services of a specialist CCTV service company who would also be considered as authorised personnel.
 - D. Subject Access Requests are dealt with in clause 10.
 - 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.

- 3.2** The Service takes a privacy by design approach and will conduct a Data Protection Impact Assessment (DPIA) with guidance from the Service's DPO in accordance with GDPR, as they are systematically monitoring and capturing 'vulnerable' data subjects, such as children. The Service will also ensure a GDPR compliant agreement is in place with any organisation where personal data/CCTV footage is processed on behalf of the Service.
- 3.3** Any changes to CCTV monitoring will be subject to a Data Protection Impact Assessment (DPIA) in which the Service's DPO will provide advice.
- 3.4** The use of CCTV recording involving audio recording between members of the public is highly intrusive and unlikely to be justified. The appropriate personnel should choose a system without this facility if possible. If CCTV system are equipped with a sound recording facility these should be disabled.
- 3.5** In the exceptional circumstances where audio recording is justified and this has been agreed with the DPO, it must be limited to that which is necessary to achieve the purposes specified in paragraph 4, appropriate signage and notification must make it clear that audio recording is or may be carried out.
- 3.6 Camera location schedule.** The Head of Systems and Processes maintains a written schedule of every camera in operation across all Service sites, including Maypole Farm. The schedule records the camera reference, its location, its field of view, whether it is internal or external, the purpose it serves, whether it records audio, and the date of its last review. The schedule is held on SharePoint, is shared with the DPO, and is updated whenever a camera is added, moved, repositioned or decommissioned. Cameras must not be aimed off Service grounds into public spaces or neighbouring private property.
- 3.7 Signage.** Clear and legible signs are displayed at every entrance and in every area covered by CCTV. Each sign identifies Tuition Extra (Kent) Ltd as the operator of the system and as the data controller, states the purpose for which the cameras are used, confirms whether audio is recorded, and provides contact details for enquiries. Signage is checked as part of the annual policy review and is produced in an accessible format appropriate to the Service's SEND cohort.
- 3.8 Named roles.** For the avoidance of doubt, the following named roles apply under this Policy. The Data Protection Officer is Emma Sedgwick (emma.sedgwick@tuition-extra.co.uk). The System Manager, responsible for the day-to-day operation, maintenance and security of the CCTV system, is the Head of Systems and Processes, Jean-Paul Muller. The CEO, Ruth Minhall, holds ultimate accountability for the operation of the system. Enquiries about the CCTV system should be directed to the Head of Systems and Processes. References in this Policy to a "governing body" should be read as references to the Executive Board, and references to the "head of service/school" as references to the CEO or the relevant Head of Site.
- 3.9 Suppliers and processors.** Where a maintenance provider, installer or hosting provider processes CCTV footage on the Service's behalf, that supplier is a data processor. A written data processing agreement compliant with Article 28 of the UK GDPR must be in place before any access is granted. The Service records the identity of each such supplier, the location in which footage is stored, the retention applied, any sub-processors used, and the security measures in place. Remote access by a

supplier must be time-limited, individually authorised, supervised by the System Manager and recorded on the CCTV Access Log.

3.10

S

afeguarding. Where CCTV footage concerns, or may concern, the welfare of a child, the Designated Safeguarding Lead must be involved from the outset and the matter handled in accordance with the Service's Child Protection and Safeguarding Policy and Keeping Children Safe in Education. Safeguarding always takes precedence. Footage that forms part of a safeguarding record is retained in line with the safeguarding retention schedule rather than the 30-day CCTV retention period, and is stored within approved Service systems only.

3.11 DPIA review cycle. The Data Protection Impact Assessment for the CCTV system is reviewed at least annually, and in every case before a camera is added, moved or upgraded, before the system is replaced, and before any change to retention or to the purposes for which footage is used. Those most likely to be affected, including pupils, parents and carers, staff and neighbouring residents, are consulted as part of the assessment where it is proportionate to do so. Any risk identified is addressed and the mitigation recorded.

4. OBJECTIVES OF THE CCTV SYSTEM

To protect pupils, staff and visitors.

- 4.1** To increase personal safety and reduce the fear of crime.
- 4.2** To protect the service buildings and assets.
- 4.3** Without prejudice, to protect the personal property of pupils, staff and visitors.
- 4.4** To support the police in preventing and detecting crime.
- 4.5** To assist in identifying, apprehending and prosecuting offenders.
- 4.6** To assist in managing the Service.

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. Only individuals with specific written authority from the head of service/school may view CCTV footage. All access for viewing recorded footage must be logged, a suggested log is included in this policy.

5.2 In general, CCTV footage is retained for 30 days and is then overwritten automatically by the recording system, unless an incident has occurred on Service premises and the footage is to be kept for a purpose. CCTV footage is stored securely in a lockable office / on

the Service's password protected software system. If an incident has occurred, the footage in question should be stored securely in a way that maintains the integrity of the images pending further action. Any decision to retain footage beyond 30 days must be authorised in writing by the CEO or the Head of Systems and Processes, notified to the DPO, and recorded on the CCTV Access Log with the reason, the review date and the person accountable for the extended retention. Once the action/investigation has been concluded, a review of the retention of the footage should be exercised and secure, permanent disposal of the footage should occur where there is no longer a valid lawful basis to keep the images.

5.3 The Service 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 Service'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

5.4 The System Manager is responsible for the security of the CCTV system and of the footage it produces. The following controls apply as a minimum. All default manufacturer passwords on cameras, recorders and network video recorders must be changed before the equipment is brought into service, and credentials must meet the standards set out in the Service's Data Protection and Cyber Security Policies. Multi-factor authentication is enabled on any cloud-hosted or remotely accessible element of the system. Access is granted on a named, role-based basis and is revoked promptly when a member of staff leaves or changes role. Footage is encrypted in transit and at rest wherever the system supports it, and any exported footage is encrypted or password protected. The CCTV system is segregated from the general staff network so far as is reasonably practicable, and is not exposed directly to the internet. Firmware and software security updates are applied promptly. Visual display monitors are positioned so that only authorised personnel can see them.

5.5 The System Manager carries out a documented check of the system each term, and the DPO reviews the outcome. That check confirms that all cameras are functioning and correctly positioned, that image quality remains sufficient for the purposes of the system, that date and time stamps are accurate (including after the clocks change), that footage is being deleted automatically at the end of the retention period, that access permissions remain appropriate, and that the CCTV Access Log has been completed correctly. Faults are reported and remedied as soon as reasonably practicable, and any fault affecting the

security of footage is treated as a potential personal data breach and reported to the DPO immediately.

6. DISCLOSURE OF IMAGES

6.1 The Service 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. Any disclosure should be clearly documented by the Service as outlined in clause 5.3.

6.2 There will be no disclosure of recorded data to third parties without a lawful basis. It is acceptable for the Service to disclose images to law enforcement agencies for the purpose of prevention and detection of crime. These requests should be:

- be provided in writing (WA170) where possible
- signed by authorised officers
- make reference to the name and section of the legislation that entitles them to receive the information.

6.3 The Service 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 process will remain the same when disclosing in regard to insurance purposes. 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 given to the authorised recipient separately from the email containing the recording, ensuring that the original copy of the recording is kept at the Service for only as long as is necessary for the purpose of retaining the recording.

- If the immediate viewing of a recording is necessary, this will be governed by clause 5 above.
- 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. Where technology permits, images of third parties should be blurred and unidentifiable if a disclosure request does not pertain to them.
- The data may be used within the service'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 The persons authorised to operate the equipment and view the monitors are appropriate personnel. The appropriate personnel will have received training in the operation of the particular systems used by the Service. 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 On occasion the Service may receive a request to carry out covert monitoring on behalf of the Police, which must be requested with evidence of the Police's RIPA authorisation for this surveillance. Where the Police state that they cannot produce that authorisation because of the sensitivity of the investigation, the request must be escalated to the CEO and the DPO, who will decide whether there is a lawful basis to proceed and will record the decision and the reasons for it in writing. No covert monitoring may begin without that written authorisation.

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

7.4 Covert surveillance means the operation of cameras in a place where people have not been made aware that they are under surveillance. The Service will use covert surveillance only in exceptional circumstances, where there are reasonable grounds to suspect criminal activity or serious misconduct and where informing the individuals concerned would prejudice the investigation. Covert surveillance must never be used in an area where individuals have a heightened expectation of privacy. Before any covert surveillance begins it must be authorised in writing by the CEO on the advice of the DPO, supported by a Data Protection Impact Assessment, and where a child may be affected it must additionally be approved by the Designated Safeguarding Lead. Authorisation must specify the purpose, the areas covered, the individuals likely to be affected and a defined end date, and must be reviewed at intervals of no more than four weeks. Covert surveillance must cease as soon as the investigation concludes. A record of every authorisation, review and outcome is kept by the DPO.

8. BREACHES

8.1 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.

8.2 Any breach of security will be initially investigated by the Service's appropriate personnel, in order to discuss this further with the Service's DPO, governing body and Senior Leadership Team. The Service'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 Service'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.

8.3 The Service may take the appropriate disciplinary action in the relevant circumstances. A breach of this policy will be governed by the Service's existing policies and procedures. Any serious breach of the CCTV Policy 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 Service's DPO.

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

** Where a criminal offence has been committed on Service premises, the Service 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 Service 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 Service's website and send it to the Service'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 Service's email address to be dealt with during normal office hours.

9. CCTV and GDPR

9.1 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 service uses CCTV cameras. Visitors must have the knowledge of who to contact to make an enquiry regarding the system where this is not obvious.

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

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

9.4. The right to rectification will apply where possible.

9.5 The right to data portability is not applicable as CCTV is not processed by automated means on the basis of consent or contract. Automated decision making is not included in this process. Because the Service relies on legitimate interests, individuals have an absolute right to object under Article 21 of the UK GDPR; the Service will cease processing unless it can demonstrate compelling legitimate grounds which override the individual's interests, rights and freedoms. Each objection is considered on its merits and recorded, with DPO advice.

9.6 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.

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

9.8 All rights can be exercised by individuals contacting the Service or the named DPO.

10. SUBJECT ACCESS REQUESTS

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

10.2 A request may be made in any form, verbally or in writing, and need not use any particular wording or refer to any legislation. All staff are trained to recognise a subject access request and must forward it to the DPO immediately. Requests made in writing can usually be dealt with more quickly. 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. In accordance with Article 15(1A) of the UK GDPR, as inserted by the Data (Use and Access) Act 2025, the Service is required to carry out only a reasonable and proportionate search for footage. Where a request is not sufficiently specific to enable the footage to be located, or where the Service needs to verify the requester's identity, the Service may ask for the further information it reasonably requires. The time limit for responding is paused from the date that request is made until the date the necessary information is received (the "stop the clock" provision).

10.3 Where a child is the data subject, the personal data belongs to the child and not to their parent or carer. A parent or carer may make a request on a child's behalf only where the child is unable to understand their rights and the implications of the request, or where the child has given their consent. Maturity is assessed case by case, with the DPO's advice, and with particular care given the SEND profile of the Service's pupils. This clause is to be applied consistently with the Service's Data Protection Policy.

10.4 The Service will respond to a request within one calendar month of receiving a valid request. That period runs from the date the request was received or, where identification or clarification is required, from the date the necessary information is provided. Where a request is complex or where a number of requests have been received, the Service may extend the period by up to a further two months. The Service will inform the requester of

any extension, and the reasons for it, within one month of receiving the request. Requests are not refused as unfounded or excessive without the DPO's advice, and the reasons for any refusal are recorded.

10.5 Where a Subject Access Request includes footage of another individual not included in the request, the service 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.

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

10.7 Wherever possible, the Service will notify the requester if an exemption or limitation to their request applies, such as, but not limited to:

- **10.7.1** A claim to legal professional privilege – the Data (Use and Access) Act 2025 provides an express exemption from the right of access for information in respect of which a claim to legal professional privilege could be maintained
- **10.7.2** The request will infringe on a third party's rights and freedoms
- **10.7.3** Any other exemption to the right of access as stated in the GDPR and DPA.

10.8 The Service understands that individuals have further individual rights under the GDPR and DPA and will seek DPO advice where necessary.

11 INFORMATION REQUESTS FROM COMMISSIONING AND PUBLIC BODIES

11.1 Tuition Extra (Kent) Ltd is a private company and is not a public authority listed in Schedule 1 to the Freedom of Information Act 2000. The Service is not therefore subject to the Freedom of Information Act and does not accept or process requests made under it. Any request received purporting to be an FOI request will be acknowledged, the requester will be told that the Act does not apply to the Service, and the request will be considered instead, where appropriate, as a subject access request under section 10 of this Policy.

11.2 The Service may, however, receive requests for CCTV footage from Kent County Council or from another local authority or public body under its commissioning, placement or safeguarding arrangements. Such requests are not FOI requests. They will be referred to the DPO and disclosed only where there is a lawful basis to do so, in accordance with section 6 of this Policy, limited to the minimum footage necessary, and recorded on the CCTV Access Log. Where individuals are capable of being identified from the footage, the rights and freedoms of those individuals must be considered before any disclosure is made, and third parties obscured where the request does not pertain to them.

12 APPEALS

12.1 There is a Service '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 document will be provided to the requester in the final response from the Service to the individual making the Subject Access Request.

13 COMPLAINTS

13.1 Complaints and enquiries about the operation of CCTV within the service should be addressed through the Service's complaints procedure. Where necessary, the Service's Data Protection Officer will be informed of the complaint. Separately, under section 164A of the Data Protection Act 2018, as inserted by the Data (Use and Access) Act 2025 and applying to the Service from 19 June 2026, individuals have a statutory right to complain directly to the Service about how their personal data, including CCTV footage, has been handled. A complaint of this kind may be made to the Data Protection Officer, Emma Sedgwick, at emma.sedgwick@tuition-extra.co.uk, or by any other reasonable means including in person or by telephone, and need not use any particular form of words or cite any legislation. Where such a complaint is received the Service will acknowledge receipt within 30 days, investigate and respond without undue delay, keep the complainant informed of progress, and notify them of the outcome. Complaints from children will be handled in clear, age-appropriate language. A record of all data protection complaints and their outcomes is maintained by the DPO. Individuals retain the right to complain to the Information Commissioner's Office at any time, and the Service will tell them how to do so.

14 REVIEW

14.1 The Service's DPO and SLT will review this document annually to reflect changes in best practice, legislative changes and guidance from the Regulatory Authority (Information Commissioner's Office). The annual review will consider expressly whether the continued use of each camera remains necessary, proportionate and effective in meeting the objectives set out in section 4, and whether any camera should be repositioned or decommissioned. The review will also confirm that the Legitimate Interests Assessment, the Data Protection Impact Assessment, the Appropriate Policy Document, the camera location schedule and the privacy notices remain accurate and up to date. A review will additionally be triggered by any significant legislative or regulatory change, by any personal data breach involving CCTV, and by any material change to the system. The outcome of each review is reported to the Executive Board.

School / Education Service CCTV SYSTEM ACCESS LOG

This form is designed to ensure compliance with relevant UK data protection legislation, specifically the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA 2018)**, by maintaining an accurate audit log of access to personal data (which CCTV footage often contains).

This log must be completed **every time** a member of staff accesses the CCTV system for viewing, playback, export, or any other purpose. This is a mandatory requirement under the school's Data Protection and CCTV Policy.

School/Service Name: Tuition Extra (Kent) Ltd to include Maypole Farm
Log Date:

SECTION A: Requester & Authorisation Details

Field	Detail
Staff Member Name (Requester):	
Staff Member Role/Title:	
Staff Signature:	
Date & Time of Access:	Date: Time:

Authorising Manager/Personnel (Print Name): (Must be a Senior Leader, or designated security admin)	
Authorising Manager/Personnel Signature:	

SECTION B: Purpose of Access

Please tick the primary reason for accessing the footage. If "Other," please specify.

Purpose	Tick ()	Details (Brief Explanation Required)
Safety Incident Investigation: (e.g., student/staff injury, accident)		
Disciplinary Investigation: (e.g., staff misconduct, policy breach)		
Theft/Vandalism Investigation:		
General Security Monitoring: (Requires high-level justification)		
Testing/Maintenance of System: (Requires sign-off by Head of Systems)		

Law Enforcement Request: (Requires formal DPA 2018 Schedule 2, Part 1, paragraph 2 (crime and taxation) exemption justification)		
Subject Access Request (SAR): (Requires formal SAR process and DPO sign-off)		
Other (Specify):		

Full description of the incident/reason for access:

(Be specific, e.g., "Investigating a reported fall outside the main hall at approximately 10:15 am.")

SECTION C: Footage Details & Action Taken

Field	Detail
Date Range of Footage Accessed:	From: To:
Time Range of Footage Accessed:	From: To:
Specific Camera Location(s) Accessed: (e.g., 'Main Hall Entrance Cam 3', 'Car Park North')	

Action Taken: (Tick all that apply)	Viewed ☐ Only ☐ Downloaded/Exported ☐ Copied to External Media ☐ Deleted/Archived ☐
If Footage Downloaded/Exported: (File name and Storage location, e.g., 'Incident_Main_Hall_20250901.mp4' on secure network folder '/Security/IncidentLogs')	
Duration of Access Session:	From: To:

SECTION D: Data Protection Compliance Declaration

I, the undersigned, confirm that:

1. I have accessed the CCTV system strictly for the purpose outlined in Section B.
2. I understand that the footage contains personal data and must be treated in accordance with the school's **CCTV Policy, Data Protection Policy**, and the **UK GDPR/DPA 2018**.
3. Any footage downloaded or exported will be stored securely, only accessed by authorised personnel, and retained only for the necessary period as defined by the school's retention schedule.
4. I will report any misuse or breach of this footage immediately to the Data Protection Officer (DPO).

Staff Member (Requester) Name:

Date:

Form Management Notes for the Administrator (Do not print on circulated form)

- **Retention:** Keep completed forms in a secure, locked location (physical or digital). The retention period for this log should align with the retention

period for other data breach or incident logs (often 6 years, but check school policy).

- **Audit Trail:** This log is the mandatory audit trail for all CCTV access. It is vital evidence in the event of a regulatory inquiry or data subject complaint.
- **DPO:** Ensure the school's Data Protection Officer (DPO) is aware of, and approves, the use and storage of this log.
- **Training:** All staff who may require access to the CCTV system must be trained on the correct procedure and the importance of completing this log accurately.