# STANWIX SCHOOL

## Together we learn, Together we grow, Together we thrive

# SURVEILLANCE CAMERA PROCEDURES

| **Approved by** | | | |
|---|---|---|---|
| **Name:** | Fiona Manuel | | |
| **Position:** | Chair of Trustees | | |
| **Signed:** | On File | | |
| **Date** | March 2026 | **Version No:** | **7** |
| **Review date:** | March 2027 | | |

# REVIEW SHEET

**Each entry in the table below summarises the changes to this Policy and procedures made since the last review (if any).**

| Version Number | KAHSC Version Description | Date of Revision/Reviewed |
|---|---|---|
| 1 | Original | Sept 2012 |
| 2 | Significant rewrite in line with the ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015) | Sept 2015 |
| 3 | Minor amendment. | Feb 2016 |
| 4 | Significant re-write in light of digital technologies and the new Data Protection Act 2018 with improved reference to the latest Information Commissioner's Office (ICO) guidance. The aim is to keep the procedures short and user friendly but still enable good decision-making through signposting to official guidance. | Sept 2018 |
| 5 | Reviewed – links checked and amended | Oct 2019 |
| 6 | Updated language to reflect absorption of the ICO CCTV Code of Practice into general ICO advice and the broadening of it to reflect the Home Office Surveillance Camera Code of Practice covering surveillance such as ANPR, drones, AI controlled systems, and emerging technologies like facial recognition. Checked and updated links. Removed all appendices (a sign template and an audit form) to make them links to separate documents for ease of use and distribution. | Sept 2022 |
| 7 | Links to the new KAHub inserted. No other changes. | Sept 2023 |
| | Reviewed - no changes to content | Nov 2024 |
| 8 | Minor changes to broken links | Sept 2025 |

# CONTENTS


**1. Definitions, References and Useful Links ..... 1**

**2. Introduction ..... 1**

**3. Description & objectives of the surveillance system ..... 2**

3.1 System and equipment ..... 2

3.2 Camera siting ..... 2

3.3 Notification and signage ..... 3

**4. Management roles and responsibilities ..... 3**

4.1 The Head teacher or manager ..... 3

4.2 The System Manager ..... 4

4.3 The Data Protection Officer (DPO) ..... 4

4.4 Surveillance System Operators ..... 4

4.5 Security companies ..... **Error! Bookmark not defined.**

**5. System operation ..... 4**

5.1 Live visual feeds and data recording ..... 4

5.2 Live audio feeds and data recording ..... 5

5.3 Covert surveillance ..... 5

5.4 Control room operations ..... 5

**6. Surveillance data handling ..... 6**

6.1 Storage ..... 6

6.2 Retention ..... 7

6.3 Access & disclosure ..... 7

6.4 Subject access requests (SARs) ..... 7

6.5 Freedom of information (FOI) requests ..... 8

**7. Breaches ..... 9**

**8. Monitoring and review ..... 9**

**9. Complaints ..... 9**

*This page is intentionally blank for printing purposes*

# SURVEILLANCE CAMERA PROCEDURES

## 1. Definitions, References and Useful Links

| | |
|---|---|
| **Data controller:** | Usually an organisation rather than a person, that determines the purpose and means of processing personal data. |
| **Data processing:** | Anything that is done with data e.g. recording, displaying, using, changing, storing, transferring, deleting etc. |
| **'Data Protection by Design':** | The integration of appropriate technical and organisational measures to protect personal data and an individual's right to privacy from the design stage throughout the whole life cycle of the data. |
| **Data subject:** | Anyone who is the subject of data we hold i.e. any person whose image we record using our surveillance cameras. |
| **Personal data:** | Any data that can be used to, directly or indirectly, identify a living person i.e. their image. |
| **Surveillance Camera/system** | Traditional Closed-Circuit Television (CCTV) systems, Automatic Numberplate Recognition (ABPR) systems, Artificial Intelligence controlled systems, body-worn cameras, and unmanned aerial systems (drones). |
| **Operator:** | A member of staff who has received specific training in operating surveillance systems. |

In developing our Surveillance Camera Procedures, we had due regard for legislation, statutory and non-statutory guidance as follows:

- The Information Commissioner's Office (ICO) guidance regarding:
  - Right of access | ICO (handling a Subject Access Request or SAR),
  - Video surveillance | ICO,
  - Data Protection Impact Assessments (DPIAs) | ICO, and
- The Regulation of Investigatory Powers Act (RIPA, 2000)
- The Protection of Freedoms Act (POFA, 2012)
- The Data Protection Act (DPA, 2018)
- The Human Rights Act (HRA, 1998)
- The Equality Act (EA, 2010)
- The Home Office guidance: Surveillance Camera Code of Practice
- Our Data Protection Policy and associated procedures.

## 2. Introduction

This school has in place a surveillance camera system that operates, both inside and outside of the buildings. It is a secure system of video cameras which transmits a signal to a specific place for display on limited monitoring devices and which can be recorded

We recognise that our system collects personal data that is regulated by the UK General Data Protection Regulation (UK GDPR) alongside the Data Protection Act (DPA) 2018. These procedures detail the purpose, use and management of the system and how we will ensure that we comply with relevant legislation and safeguard the individual rights of our data subjects.

Our school is registered with the ICO as a Data Controller, our registration is updated annually, and it includes our surveillance system. ICO Registration Number: 00013163601.

The individual named as responsible for the operation of the system is Darren Glynn, Headteacher) Anyone who wants to discuss our use of surveillance and the guidelines we follow can contact them on

01228 596069 and/or office@stanwix.cumbria.sch.uk during normal working hours.

We also have a Data Protection Officer, Gerard Barr, whose contact details can be requested through the school office office@cumbria.sch.uk so that anyone can easily raise any concerns they might have about our use of personal data, including our surveillance system.

In operating surveillance we will follow, and staff should refer to Video surveillance | ICO guidance. It may also be necessary to refer to our Data Protection Policy e.g. to guide the protection of transfers of surveillance data.

These Procedures will be subject to regular review. If a new or additional system is being considered, the review will involve a 'Data Protection by Design' approach using a Data Protection Impact Assessment (DPIA) including consultation with the affected school community e.g. staff, students, parents etc. where appropriate.

Our aim is to ensure we avoid recording and storing excessive amounts of personal data.

## 3. Description & objectives of the surveillance system

The surveillance system comprises 14 fixed and moving cameras without sound recordings located around the site both internally and externally which function 24 hours a day throughout the year for the purposes of:

- protecting the buildings, assets, and personal property on site.
- enhancing the personal safety of staff, students, and members of the public such as visitors.
- reducing the fear and potential incidence of crime including theft and vandalism.
- reducing the fear and potential incidence of anti-social and harmful behaviours like bullying or hate crimes.
- supporting the Police in order to deter and detect crime.
- assisting in identifying, apprehending, and prosecuting offenders; and
- ensuring that site rules are respected so that the school can be properly managed.

### 3.1 System and equipment

When we decided what system to install, we chose one that can produce clear images which are useful for our purposes e.g. a large enough viewing area, high enough resolution, and sufficient frames per second of movement to be able to identify undesirable behaviour and the perpetrators. We also made sure we have the technology to compress and share the data with the proper authorities such as the Police without negatively affecting the quality of recordings and therefore its usefulness.

If we need to further update or change our surveillance system, we will use the Surveillance Camera Commissioner's buyer's toolkit - GOV.UK to help us maintain compliance.

We regularly review our use of surveillance, and we can change the way it operates, if necessary, to better protect people's privacy. For example: we can make it so that certain cameras record only at certain times of day when we have identified that the problem we need to monitor occurs and not at times when we know it doesn't.

### 3.2 Camera siting

When deciding where to put cameras, we tried to put them in plain sight and in places where they can capture clear images of the spaces we need to monitor, while avoiding the capture of any images (or any clear images) of people who are not using or visiting our premises e.g. passers-by or the gardens, driveways etc. of our neighbours.

Surveillance of public areas may include corridors, reception area and outside playgrounds.

- **Protection of buildings, assets, property, and personal property:** at building perimeters, entrances & exits, lobbies & corridors, special storage areas, cashier locations, receiving areas for goods/services.
- **Monitoring of access control systems:** on restricted access areas, especially the main entrance where the camera works in tandem with the intercom so reception staff can see who is at the door, or ANPR cameras to control parking or community access.

- **Verification of security alarms:** at intrusion alarms points, exit door controls, external alarms.
- **Video patrol of public areas:** on parking areas, main entrance/exit gates, traffic control areas.
- **Providing evidence for internal disciplinary action or external criminal investigation (carried out by the Police):** surveillance of misconduct, bullying and other undesirable behaviours; robbery, burglary, and theft surveillance.

No moving camera is sited in any area where it can capture clear images of unintended or overlooked spaces when an operator moves it. Cameras are also never sited anywhere that people have a reasonable expectation of privacy e.g. toilets and changing rooms.

We also considered how the location environment might affect recording quality e.g. too much or too little daylight; insufficient night-time illumination; plant growth or summer foliage obscuring the lens; vulnerability to vandalism etc.

### 3.3 Notification and signage

These surveillance procedures describe the purpose and location of surveillance and include the contact details for the system manager in the Introduction so that anyone who wants to discuss our use of surveillance and the guidelines we follow can contact them.

These procedures are freely available to all staff on the secure staff-only information network. A copy can be provided on request to staff, students, parents, carers, or other visitors.

Our community and the general public are made aware of the presence of surveillance by appropriate signage at the entrance to a surveillance zone and this is reinforced with further signage inside some areas. Our signs:

- are clearly visible and readable e.g. large enough to be noticed, larger print if meant to be seen from a vehicle, more prominent and/or frequent in places where people might not expect to find surveillance, or where the system is so discreet people can't easily see that they are being monitored.
- include details of the organisation that operates the system, why surveillance is being used and who to contact about the scheme (where these things are not obvious to those being monitored e.g. if we use a security company to operate our system for us).
- include basic contact details for the system manager, either a website address where contact details can be obtained or a telephone number.

## 4. Management roles and responsibilities

### 4.1 The Head teacher or manager

The head teacher or duty manager is responsible for day-to-day operations including an overview of all data protection matters. With regard to surveillance specifically, they are responsible for:

- ensuring the system in use is broadly fit for purpose and has a suitable maintenance scheme in place.
- ensuring the system is properly registered with the ICO, that people affected by surveillance are informed about it, and that processing of the data is fair, lawful, and not excessive.
- ensuring mechanisms exist to provide all staff and other relevant individuals, such as agency workers, with suitable information and/or training to enable them to follow these procedures.
- promoting the development of good data management practice, leading by example, and encouraging good information handling practice.
- authorising the release of surveillance data to any third parties.
- approving any temporary extension of the surveillance system to cover special events that have particular security or access & communication requirements and ensuring proper withdrawal afterwards. (This is not the same as approval for mobile equipment or covert surveillance being used for very serious or criminal investigations – please see Section 5.3: Covert Surveillance).

Any of these tasks can and may be delegated to other suitably competent managerial staff, but they remain a management responsibility of the head teacher or manager.

### 4.2 The System Manager

The surveillance system manager is responsible for the day-to-day running of the system to include:

- Periodic checks of the hardware and the siting of it e.g. plant growth, vandalism etc.
- Ensuring software, especially security updates are successfully applied as necessary.
- Carrying out the periodic tasks required e.g. monitoring data, checking storage arrangements are still suitable, ensuring data has been properly deleted etc.
- Keeping comprehensive and accurate records of all data, surveillance and recordings, and the processing of it, especially the storage of any data and its deletion.
- Collecting and presenting useful data to senior leaders regarding the effectiveness of the system.

This person will also be available during normal operating hours and will understand and have available to them all relevant policies, procedures, technical and security information about the surveillance system to enable them to answer queries or help solve problems.

### 4.3 The Data Protection Officer (DPO)

There is no specific role for our DPO in managing our surveillance systems. They have more general data protection responsibilities such as:

- conducting or advising on our Data Protection Impact Assessment if we want to extend our surveillance or significantly change something about how we operate it.
- raising awareness of data protection issues which might include the proper use of surveillance.
- monitoring our own monitoring (records) of our surveillance practice.
- reporting on data protection compliance to the governing body which could include the effectiveness of our surveillance; and
- reporting data protection breaches to the ICO.

Our DPO is therefore required to liaise with surveillance camera operators and the system manager to adequately support them with the data protections aspects of their work.

### 4.4 Surveillance System Operators

All surveillance system operators are members of staff suitably authorised to carry out their role and who have received specific training in:

- arrangements for recording, retaining, and deleting surveillance data in line with data protection laws.
- handling information securely.
- responding appropriately to requests for information e.g. from staff, individuals, the police etc.; and
- recognising a Subject Access Request and how to respond.

Operational expectations of surveillance camera operators are set out in Section 5: System Operation.

## 5. System operation

During normal operating hours, the surveillance scheme will be administered and managed by the head teacher & School Business Manager, in accordance with the principles and objectives expressed in these procedures, although day-to-day tasks and some key monitoring tasks will be delegated to suitable and trained individuals.

Outside normal operating hours, the site manager will administer the scheme where issues arise. Our DPO or a suitable senior leader will also be available remotely for advice.

### 5.1 Live visual feeds and data recording

Surveillance will generally operate 24 hours a day on every day of the year, and the following conditions will apply to all live feeds and data recordings.

All cameras are monitored from a central Control Room, and the data is only available to selected trained and authorised staff.

Our surveillance system will not be used to monitor normal teacher/student classroom activity.

Surveillance based on individual characteristics protected under the EA 2010 and other related legislation (race, gender, pregnancy, sexual orientation, national origin, disability etc.) is strictly prohibited. The system is in place to monitor suspicious activities and not individual characteristics.

Monitoring for the purposes of security and personal safety will be conducted in a professional, ethical, and legal manner and any diversion of the use of surveillance technologies and personnel for other purposes is prohibited e.g. the monitoring of political or religious activities, or monitoring employee and/or student interactions for reasons that are not compatible with those clear security and safety objectives.

Unless an immediate response to events is required, operators will not direct surveillance cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the RIPA 2000 (see Section 5.3).

When a surveillance camera zoom facility is being used, a second person will be present with the camera operator to best ensure that there is no unwarranted invasion of privacy.

Materials or knowledge secured as a result of surveillance will only be used for the purposes of ensuring security and personal safety. Data will only be published in the course of the legitimate investigation of a specific crime, and this will normally be on the advice of law enforcement or another relevant public authority. Data will never be released in any medium for the purposes of entertainment.

Information obtained through the surveillance system may only be released when authorised by the head teacher/manager following consultation with the Chair of the Trustees. Any requests for surveillance data from the Police will be fully recorded. If a law enforcement authority is seeking a recording for a specific investigation, the request must be made in writing.

## 5.2 Live audio feeds and data recording

Recording conversations between people, especially members of the public, is highly intrusive data monitoring and not something easily justified. Our surveillance system is not capable of audio recording.

## 5.3 Covert surveillance

The UK Home Office 'Covert Surveillance and Property Interference Code of Practice' (Aug 2018) paragraph 2.3 says that, "surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place".

Directed surveillance at particular individuals in a covert manner is not something we will engage in except in exceptional circumstances where serious or serial criminal offences are being committed which carry a maximum penalty of at least 6 months imprisonment. We must act in accordance with the RIPA 2000. It is much more likely that we will cooperate fully with any covert surveillance the police or other appropriate public authority receives the proper court authorisation to carry out involving our premises or organisation e.g. if serious fraud was being perpetrated against us.

We will seek appropriate advice before becoming involved in any RIPA related actions.

## 5.4 Control room operations

The viewing of live surveillance feeds is restricted to specific trained staff in a 'staff only' access area when the display includes footage of areas which are **not** in plain sight of people who can see the feed display monitor

- areas in plain sight of any untrained or unauthorised person who can also see the feed display our visitors may see the playground entrance from the gate on the monitor in reception, but they cannot see anything that they could not see if they looked around them.

**Control room operations will include:**

- A daily check on the efficiency of the system, in particular that equipment, including software updates and the means to raise the alarm in an emergency or other relevant incident, is working properly.

- Ensuring cameras are not directed at individuals, their property, or a specific group of individuals unless in direct response to unfolding events to better achieve system aims e.g. enhanced safety and security by identifying issues and the people involved.
- Administrative functions like maintaining secure data streams and adequate recording space, filing and maintaining incident and system maintenance logs.
- Following strict protocols when allowing normally unauthorised persons e.g. untrained staff, contractors or visitors, entry to the control room as follows:
    - Being satisfied about the control room visitor's identity and legitimate reasons for entry e.g. an untrained member of staff receiving training; a contractor carrying out servicing and maintenance work; a visitor who has been granted permission to view specific images of themselves; a parent who is being shown evidence of an incident involving their child; a police officer involved in a criminal investigation using the data; another representative with legitimate reason e.g. from the Department for Education, the Health & Safety Executive etc.
    - Refusing access to unauthorised persons when their identity or legitimate reasons are in doubt.
    - Adequately supervising control room visitors throughout their visit.
    - Keeping a record of all control room visitors in the logbook including visits by normally unauthorised staff (visitor name, date & time of entry and exit, reason for entry, name of operator who supervised them).
    - Adequately protecting people's data protection rights when visitors are in the control room e.g. turning live feed monitors away or off (after ensuring data not being monitored live is being recorded instead), curtailing the visit if circumstances demand it.

The control room will always have at least one trained operator in it, or it will be locked.

Recordings will only be made by authorised staff who will only make them available for viewing by authorised staff, authorised visitors, or an appropriate public authority, in the control room or in another suitable and restricted area, such as a secure office.

## 6. Surveillance data handling

### 6.1 Storage

Surveillance data storage facilities have been designed to ensure the integrity of the data being stored is maintained so it can be used effectively for its intended purpose i.e. storage arrangements do not significantly degrade the data making it less useful.

We adequately protect this data using a mixture of operational security measures such as restricting access to trained/authorised users and locking areas where it is stored or can be viewed, and technical security measures such as encryption, secure networks and personal logins that are never shared. We also keep records of routine access through the system's own performance monitoring logs, and records of non-routine systems access via the logbook.

Surveillance camera operators receive training in data protection relevant to their specific role and all staff can find information about their responsibilities in our Data Protection Policy. All staff and relevant others such as contractors are made aware and reminded regularly that misuse of our surveillance may result in disciplinary and/or criminal proceedings against them.

Any storage of surveillance data on any kind of removable media e.g. tapes, DVDs, USB devices etc. is strictly controlled with checks in place to ensure that it:

- can only be done by a trained operative.
- does not interrupt normal surveillance operations.
- does not degrade the data or remove important date and time stamping.
- provides the information in a suitable format which is straightforward to use.
- is recorded in the automatic or manual logbook, including the final destination where ownership of the record or a copy of the record has passed to a third party e.g. police, the person in the images etc.
- is appropriately and securely stored, including sealed against tampering if being kept as evidence in any kind of proceedings.

When recording or transferring surveillance data to removable media:

- Each device will be marked with a unique reference point to easily identify it from any other.
- Each device will be suitably wiped clean of any previous data *before* subsequent recordings are transferred to it.
- Devices or data files on a device will be appropriately marked with start and end times and dates and any other important information such as camera reference/location etc.
- Devices required for evidential purposes will be appropriately sealed against tampering in front of a suitable witness, signed off by the system manager or head teacher on behalf of our organisation as the data controller, and stored securely but separately from other recordings in readiness for handover to the proper authorities.
- When surveillance data has been sealed, it can be unsealed provided there is good reason e.g. a copy needs to be made for handover to the police – this unsealing must be done in front of an appropriate witness who is present until the original data is resealed and an appropriate record has been made in the logbook which includes details of the witness.
- Any copies made for evidential purposes will be handed over to the proper authorities at the earliest opportunity and a copy retained until the conclusion of any legal action.

## 6.2 Retention

Legislation requires that personal data only be kept for as long as is necessary to achieve the outcomes that it was processed for in the first place. It does not dictate how long we can retain data such as surveillance camera recordings, and we only need to have a clear and justifiable policy decision to keep it.

Our retention schedule has some flexibility in it and is determined by:

- the purpose for which the information is being collected and how long it is needed to achieve this purpose.
- the settings we have selected for routine and automatic deletion, currently 28 days on the basis of how long it has taken in the past to discover, properly investigate and deal with issues.
- our procedure for temporarily extending the retention period in a routine way, for example, over the entire summer holiday period to ensure surveillance remains effective at a potentially risky time of year for the premises.
- what appropriate public authorities such as the police require us to retain and for how long in the interests of a criminal prosecution.

When we review this retention schedule, we will look at our current practice and ask:

- Have we decided on the shortest possible retention period based on our reasons for keeping data?
- Do all relevant staff, especially the surveillance camera operators or system manager, understand our retention schedule?
- Are measures in place to ensure the permanent deletion of information through secure methods at the end of this period?
- Are the checks we carry out systematic and do they include compliance with the retention period in practice?

Retention is a key question in the annual system review (see Contents Page for a link to a record sheet).

## 6.3 Access & disclosure

Surveillance data is protected against unauthorised access through appropriate organisational and technical security measures, in accordance with the Data Protection Act 2018 and all relevant statutory guidance.

Access to live or recorded surveillance footage is restricted to trained and authorised personnel. Footage will only be viewed or used for purposes consistent with the original reason for installation of the system, including safeguarding, site security, the prevention or detection of crime, or to meet legal obligations and individuals' rights under the Data Protection Act 2018. Further information is set out in our Data Protection Policy.

Any request for access to surveillance data from individuals who are not normally authorised to view it must be made in writing. All requests will be assessed on a case-by-case basis and the decision, whether approved or refused, will be formally recorded with reasons. Disclosure will only take place where there is a clear lawful basis, including where required for the prevention or detection of crime, safeguarding, legal proceedings, insurance matters, or in response to a valid Subject Access Request.

Where footage contains images of individuals other than the requester, including pupils, access will only be granted where it is lawful, necessary and proportionate to do so. We will take reasonable steps to protect the privacy, data protection and safeguarding rights of third parties. This may include redaction, supervised viewing, provision of edited footage, or refusal of access where adequate protection cannot be achieved.

Copies of footage will only be provided were lawful and necessary. Any disclosure will be limited to relevant material and transferred securely, with appropriate measures taken to preserve confidentiality and evidential integrity. We reserve the right to refuse any request that does not comply with the Data Protection Act 2018 or other applicable legislation, except where disclosure is mandated by a court order or other legal requirement.

Internal requests will be considered and recorded by the system manager in line with their training and delegated authority. Requests from external parties must be authorised and signed off by the Head Teacher or an appropriately designated senior leader.

Where information is disclosed to a public authority, such as the police or a court, the recipient becomes responsible for compliance with applicable legislation, including the Data Protection Act 2018 and the Human Rights Act 1998, in relation to their use and any onward disclosure.

Surveillance data will not be released to the internet. Any public release for identification purposes will only take place by, or under the explicit written direction of, a lawful authority.

All processing and disclosure of surveillance data will be conducted in accordance with statutory requirements, relevant codes of practice, and guidance issued by the Information Commissioner's Office.

## 6.4 Subject access requests (SARs)

Our surveillance system and the management of it have been designed to take into account that we may need to comply with a SAR e.g. how easily data can be located, retrieved, transferred etc. Surveillance camera operators have been trained to recognise and respond appropriately to a SAR.

Where a SAR is made involving surveillance footage it is now much less likely that images which include other people can be provided to individuals due to the difficulties there might be in adequately anonymising those other people. The update to legislation as a result of the UK GDPR draws a distinction between being able to identify someone directly from the data provided, but also being able to identify someone indirectly from the data provided together with other knowledge that people who see that data might reasonably already have or come by. Pixelating the features of an individual will not necessarily obscure their identity from people who know them very well, blurring an image may not sufficiently disguise a distinctive piece of clothing worn by a known associate etc. We understand how important it is that in upholding an individual's data protection rights, we don't breach the rights of anyone else.

Details of our full procedures for handling SARs can be found in our Data Protection Policy

## 6.5 Freedom of information (FOI) requests

The Freedom of Information Act (FOIA) 2000 applies to us and we have a member of staff who understands our responsibilities and is responsible for responding to FOI requests within the 20 working days allowed from receipt of the request.

Section 40 of the FOIA contains a two-part exemption relating to information about individuals. If we receive a request for surveillance system information, we will consider:

- Whether the information is the personal data of the person requesting it. If so, that information is exempt from the FOIA. Instead, this request should be treated as a data protection Subject Access Request (please see Section 6.4 above and our Data Protection Policy for more information about handling SARs).
- Whether the information is the personal data of other people. If it is, the information can only be disclosed if to do so would not then be a breach of the DPA 2018.

Personal data that is not solely about the requester or is not already intentionally and lawfully published in the public domain cannot be disclosed in response to a FOI request.

Personal data which is only about the person making the FOI request can be disclosed to them but never as a response to an FOI request. We will inform the enquirer that we cannot process their FOI request because the data they have asked for is personal and disclosure is not permitted under the FOIA, but that as the images are only of them, the information could be provided under the DPA 2018 provisions for individuals to make a SAR of any organisation which they think holds data about them.

## 7. Breaches

A breach of these procedures by staff, and in some cases students or others, *may* result in disciplinary action and will be thoroughly investigated by the most suitable and senior leader and/or independent investigator so that appropriate remedial and disciplinary action can be taken. Information obtained in violation of these procedures may not be used in disciplinary proceedings against an employee, or a student.

A breach of these procedures may also be a breach of our legal obligations under the UK GDPR and DPA 2018 and could be reportable to the ICO where a maximum fine of €20 million could be levied. Please refer to the relevant sections of our Data Protection Policy to find out how we handle breaches of this legislation.

## 8. Monitoring and review

Routine performance monitoring, including random operating checks, may be carried out by the Head teacher or School Business Manager.

These procedures will also be regularly reviewed, either by us internally or externally by a third party to ensure the standards established when the system was set up, are being maintained.

The 'Surveillance System Annual Review' record sheet will be used to carry out and record a periodic review, at least annually, of the system's effectiveness (see Contents Page for a link). This is so that we can ensure it is still doing what it was intended to do while adequately protecting people's rights and personal data. We will take into account the recorded results of the last review and:

- Why we need to continue using the system and how we justify data retention.
- How effective technical and organisational security measures have been at protecting the data.
- Whether information about operation of the system and how individuals can make access requests remains appropriate and available.
- Whether our commitment to required and good practice remains clear and we provide suitable information about complaining to us, complaining to our DPO, or complaining to the ICO about our data protection compliance.
- Whether our monitoring of our own compliance is sufficiently regular and provides us with useful information that helps us understand how our system is being used and how we can best protect people who are affected by its use.

If a review determines that the system's effectiveness has diminished or it no longer achieves its purpose, data processing will be stopped or appropriately modified as soon as is practicable.

## 9. Complaints

Any complaints about our surveillance system or the management of it should be addressed to the Head teacher, although anyone can also independently contact our DPO because we publish their contact details on our website.

Complaints will be investigated in accordance with our Data Protection Policy, our Complaints Procedure, and these Surveillance Camera Procedures.