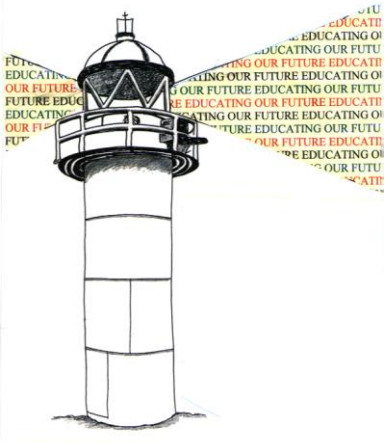

HAVERIGG PRIMARY SCHOOL

HEALTH & SAFETY POLICY - PART 3

CCTV PROCEDURES

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
1	Original	September 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)	September 2015
3	Minor amendment.	February 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.	September 2018

Using this Template (remove this text before distributing this procedure)

This Review Sheet was added to our model policies and procedures to help users quickly identify the changes we have made and how significant they are between the new and our previous version. This practice will be helpful to your own users, but your Review Sheet should reflect your versions and your changes. If this is your first use of our model, for example you would remove reference to versions 2-4 and keep only 1 which declares this version to be your original. If this is your 10th version of your procedures, you might keep our version 4 'Version Description' but label it as 'Version Number' 10.

Sections shown in ***RED TEXT*** *require settings to personalise specific parts regarding what actually happens on site or to name individuals or job titles which hold responsibility for certain tasks. Some sections may be entirely irrelevant and should be removed in full e.g. the section about security companies where one is not employed.*

To update the contents table (to remove deleted sections and update page number references), right click anywhere on the table, choose "update field" and choose the "update entire table" option.

Contents

This page is intentionally blank for printing purposes

CCTV 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 CCTV.
Personal data:	Any data that can be used to directly or indirectly identify a living person i.e. their image.
Operator:	A member of staff who has received specific training in operating CCTV systems.

In developing our CCTV Procedures we have used the following guidance and with due regard for the following pieces of legislation which affect what we do:

- The Information Commissioner's Office (ICO) website: https://ico.org.uk/ more specifically:
  - the guidance: 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data', June 17;
  - the more detailed guidance: 'Data Protection Impact Assessments (DPIAs)', and
  - the 'Subject Access Code of Practice', June 17
- 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, June 2013
- Our Data Protection Policy

2. Introduction

Haverigg Primary School (hereinafter referred to as 'the school') has in place a Closed Circuit Television (CCTV) system, inside 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 European Union's (EU) General Data Protection Regulation (GDPR) and the UK 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 CCTV system. ICO Registration Number: Z4702158.

The individual named as responsible for the operation of the system is Mrs Narongchai. Anyone who wants to discuss our use of CCTV and the guidelines we follow can contact them on 01229 772502 or admin@haverigg.cumbia.sch.uk during normal working hours.

We also have a Data Protection Officer whose contact details we publish on our website www.haverigg.cumbria.sch.uk so that anyone can easily raise any concerns they might have about our use of personal data, including our CCTV system.

In operating our CCTV we will follow the Information Commissioner's Office (ICO) guidance, *'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data', June 17*. It may also be necessary to refer to our Data Protection Policy e.g. for further guidance on protecting data transfers of CCTV images.

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 CCTV Scheme

The CCTV system comprises of seven fixed cameras without sound recordings located around the site externally only 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.

We regularly review our use of CCTV 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.

CCTV monitoring of public areas may include:

- **Protection of buildings, assets, property and personal property:** at building perimeters, entrances & exits, receiving areas for goods/services.
- **Video patrol of public areas:** on parking areas, main entrance/exit gates..
- **Providing evidence for 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 CCTV procedures describe the purpose and location of CCTV monitoring and include the contact details for the system manager in the Introduction so that anyone who wants to discuss our use of CCTV 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 CCTV 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 CCTV, 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.

A typical example warning sign for use on our premises can be found at Appendix C.

4. Management Roles and Responsibilities

4.1 The Head teacher or Manager

The Head teacher is responsible for day-to-day operations including an overview of all data protection matters. With regard to CCTV 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 the CCTV 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 CCTV data to any third parties;
- approving any temporary extension of the CCTV 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 headteacher or manager.

4.2 The System Manager

The CCTV 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 CCTV footage, and the processing of it, especially the storage of any recorded data and its deletion;
- Collecting and presenting useful data to the SLT 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 CCTV 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 CCTV 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 CCTV;
- monitoring our own monitoring (records) of our CCTV 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 therfore required to liaise with CCTV operators and the system manager to adequately support them with the data protections aspects of their work.

4.4 CCTV Operators

All CCTV 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 CCTV 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 CCTV operators are set out in Section 5: System Operation.

5. System Operation

During normal operating hours, the CCTV surveillance scheme will be administered and managed by the Head teacher 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.

CCTV 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.

5.1 Live Visual Feeds and Data Recording

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

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

CCTV monitoring 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 CCTV security technologies and personnel for other purposes is prohibited e.g. the monitoring of political or religious activities, or monitoring employee and/or student evaluations 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 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 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 CCTV monitoring 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 CCTV system may only be released when authorised by the Head teacher/Manager following consultation with the Chair of the Governing Body. Any requests for CCTV recordings/images from the Police will be fully recorded. If a law enforcement authority is seeking a recording for a specific investigation, any such request made should 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 CCTV system is not capable of audio recording.

5.3 Covert Surveillance

The UK Home Office *'Covert Surveillance and Property Interference Code of Practice' (Dec 2014)* 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" (section 1.10, p7).

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 CCTV feeds is restricted to:

- trained operators in the secure control area located – Reception desk;
- 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;

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 log book 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. CCTV Data Handling

6.1 Storage

CCTV 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 log book.

CCTV 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 CCTV may result in disciplinary and/or criminal proceedings against them.

Any storage of CCTV 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 CCTV 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 log book, 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 CCTV 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 CCTV 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 log book 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 is only 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 CCTV 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 [insert no. of 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 CCTV operators or system manager, understand our retention schedule?
- Are measures are 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 at **Appendix A**.

6.3 Access & Disclosure

CCTV data is secured against unauthorised access using a range of organisational and technical security measures and good record keeping as described in Sections 5 and 6 above.

Unless a live CCTV feed is displayed publicly and allows viewers to see only what they can see by looking around them, only trained operators and specially authorised people are permitted to view live CCTV feeds or recordings. This data can only be viewed for a reason compatible with why the system was installed in the first place, or in accordance with an individual's rights under the DPA 2018. For more information about what people's rights to data protection are and how we uphold those rights please read our Data Protection Policy.

Requests to access CCTV data from people not normally authorised to view it, including staff, must be made in writing and the decision and subsequent action recorded. Examples may include:

Example 1: to detect and prevent crime

In reporting a burglary, the headteacher provides information to the police about images of the perpetrators captured in CCTV footage.

The headteacher can invite police to the Control Room and authorised them to view the data. If they deem the data useful to their criminal investigation, a copy can be provided and the appropriate authorisation and disclosure record must be completed. If the police also request that the original data not be deleted until the conclusion of any legal proceedings, their direction on protecting the chain of evidence should be followed while they are present e.g. sealing the original media it is recorded on against tampering or adequately quarantining the original data stream from automatic system deletion and securing it against tampering with an additional security layer e.g. a file password.

Example 2: to maintain public safety

A parent asks to see the evidence on which school based disciplinary action against their child.

The headteacher can invite parents to a secure office area and authorise them to view footage of the incident which prompted the action, but it would not be appropriate to provide a copy. The footage may need to be an edited copy rather than the original to protect the privacy of individuals captured who are not already identified as being involved in the incident. The appropriate authorisation and disclosure record must be completed even where no copy of the data is provided.

Example 3: to uphold an individual's personal data rights (and potentially detect and prevent crime)

A visitor requests CCTV footage of the car park, which shows their car being damaged. They say they need it so that they, or their insurance company, can take legal action. This kind of request made by an individual is most likely to be a SAR and should be handled under those procedures outlined in our Data Protection Policy.

The headteacher should not authorise access or disclosure unless they are reasonably sure that the request is genuine and have assessed whether there is any risk to the safety of other people involved. The appropriate authorisation and disclosure record must be completed, even where a request is refused because the law requires us to justify our decisions and explain them to requestors.

Example 4: to maintain public safety (through having well trained staff)

The Assistant Headteacher with key leadership responsibility for behaviour management requests the CCTV footage of a potentially violent incident being expertly diffused by a teaching assistant to use in a whole staff meeting focussed on the development of positive behaviour management strategies.

The system manager should have received enough training to enable them to decide to agree to the request while imposing strict conditions on the use and storage of the copy made. The appropriate authorisation and disclosure record must be completed.

Example 5: to detect and prevent crime (and uphold our legal right to restitution)

Our insurance company requests CCTV footage in order to pursue a civil claim for compensation against the perpetrators of damage to school property.

The head teacher can authorise the making and secure transfer of a copy of the footage to a representative of the insurer, taking care to ensure that the identity of any person captured in the footage who was not involved in the damage is properly protected. The appropriate authorisation and disclosure record must be completed.

The decision to authorise a person to view or receive a copy of CCTV data must be made at the appropriate level. When a normally unauthorised member of staff makes a request, the system manager is expected to use their training to make and properly record an appropriate decision on allowing the access. When the requestor is not a member of staff, the headteacher must agree and sign off on the request either granting access or denying it and giving the reasons.

With the exception of any court mandated order, we have the right to reasonably refuse any request for information that we feel does not comply with the DPA 2018 and we will give our reasons.

If the data recipient is a relevant public authority e.g. the police or court, it is always the recipient's responsibility to have regard for the ICO CCTV Code of Practice and to comply with any other legal obligations such as DPA 2018, HRA 1998 etc. in relation to any further disclosures.

CCTV data will never be released onto the internet.

Information may be released to the media for identification purposes which could include release to the internet, but this will only be done by a proper law enforcement agency or under their express and written direction.

Once we have disclosed information to another body or public authority, such as the police, insurance company etc. they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA 2018 and any other relevant legislation in relation to any further disclosures.

6.4 Subject Access Requests (SAR)

Our surveillance system and the management of it has 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. CCTV operators have been trained to recognise and respond appropriately to a SAR.

Where a SAR is made involving CCTV 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 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 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.

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.

Appendix A will be used to carry out and record a periodic review, at least annually, of the system's effectiveness. 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 the ICO Code of 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 achhieves its purpose, data processing will be stopped or appropriately modified as soon as is practicable.

9. Complaints

Any complaints about our CCTV 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 CCTV Procedures.

Appendix A

CCTV SYSTEM ANNUAL REVIEW

The School has considered the need for CCTV monitoring and have decided it is necessary for the prevention and detection of crime and for the personal protection of our staff, students, visitors and other members of our community. It will not be used for other purposes. We conduct an annual review of our use of CCTV as follows.

School/Setting:		**Date:**	
Assessor:		**Signed:**	

Review Statement	Satisfactory		Problems Identified *(if any)*	Corrective Action Required *(if relevant)*	Completed By	Date Complete
	Yes	No				
Notification has been submitted to the Information Commissioner's Office and the next renewal date recorded.						
There is a named individual who is responsible for operation of the system.						
The problem we are trying to address has been clearly defined and installing cameras is the best solution.						
The CCTV system is addressing the needs and delivering the benefits that justified its use.						
The system equipment produces clear images which law enforcement (usually the police) can use to investigate crime and these can easily be taken from the system when required.						
Cameras have been sited so that they provide clear images.						
Cameras have been positioned to avoid capturing images of people who are not visiting the premises.						
There is sufficient suitable signage notifying people that CCTV monitoring is in operation, including our contact details where it might not be obvious that the system is managed by this school.						
Information is available to help deal with queries about operation of the system and how individuals can make access requests.						
Sufficient safeguards are in place to protect wireless transmission systems from interception.						
There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.						

Appendix A

Review Statement	Satisfactory		Problems Identified *(if any)*	Corrective Action Required *(if relevant)*	Completed By	Date Complete
	Yes	No				
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.						
The ability to make copies of recorded data is restricted to appropriate staff.						
Recorded data will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.						
The process for deleting data is effective and being adhered to.						
Except under the direction of an appropriate public authority (usually law enforcement), images will not be provided to third parties.						
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.						
We know how to respond to individuals making requests for copies of their own images and if we are unsure we know how to seek advice from the Information Commissioner as soon as such a request is made.						
When information is disclosed, it is transmitted as securely as possible e.g. hand delivered/collected in person on a device, a fully tracked postal service etc.						
Staff are trained in security procedures and there are sanctions in place for any misuse of surveillance system information.						
Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.						
Regular checks are carried out to ensure that the system is working properly and produces high quality and useful data.						
There is a system in place to ensure that any manufacturer recommended CCTV system and equipment updates, especially of security software are regularly sought, applied and checked as properly functioning.						
Please keep this checklist in a safe place until the date of the next Annual Review.						

Guiding Principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Source: *The Information Commissioner's Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, June 2017 (Appendix 3)*

This page is intentionally blank for printing purposes

CCTV Notice

24 hour CCTV in operation

Images are being monitored for the purposes of crime prevention and public safety.

This scheme is controlled by:

Haverigg Primary School

For more information contact:

01229 772502