Approved: __November 2019_____

Signed: _____

Review: 3 Years

Website: Yes

Heron Hill Primary School

CCTV PROCEDURES

Contents

CCTV PROCEDURES

1. Introduction

The purpose of these procedures is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Heron Hill Primary School, hereinafter referred to as 'the school'. The CCTV system is owned and operated by the school, the deployment of which is determined by the school senior leadership team.

These procedures follow the Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015); the Data Protection Act (DPA) guidelines and the School Data Protection Policy, both of which are held separately.

These procedures will be subject to regular review to include consultation as appropriate with interested parties.

1.1 Exemptions

The use of surveillance systems for limited household purposes is exempt from the DPA e.g. a video of a child in a nativity play recorded for the parent/carer's own family use is not covered by the DPA.

The use of conventional cameras (not CCTV) by the news media or for artistic purposes, such as for film making, are not covered by these procedures as an exemption within the DPA applies to activities relating to journalistic, artistic and literary purposes. See KCP Digital Images Policy.

2. Objectives of the CCTV Scheme

The system comprises a number of fixed cameras located around the site externally only for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation in the external environs of the premises during both the daytime and hours of darkness. CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and assets, both during and after school hours;
- increasing the personal safety of staff, students and visitors;
- reducing the fear of crime;
- reducing the risk of bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders;
- protecting members of the public; and
- ensuring that the school rules are respected so that the school can be properly managed.

3. General Principles

The school as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. The school owes a duty of care under the provisions of the Health and Safety at Work etc. Act, 1974 and associated legislation and utilises

CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises. The use of CCTV, and the associated images and any sound recordings is covered by the Data Protection Act 1998. These procedures outline the school's use of CCTV and how it complies with the Act. The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 can be found at https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

The Headteacher is responsible for all day-to-day data protection matters, and he will be responsible for ensuring that all members of staff and relevant individuals abide by these procedures, and for developing and encouraging good information handling within the school. Heron Hill Primary School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Notification to the ICO is renewed annually.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under these CCTV Procedures. Staff using the surveillance system or information have been trained to ensure they comply with these procedures. In particular, they have been made aware of:

- What the school's arrangements are for recording and retaining information.
- How to handle the information securely.
- What to do if they receive a request for information, for example, from the police.
- How to recognise a subject access request and what to do if they receive one.

Monitoring for security purposes 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. monitoring of political or religious activities, or employee and/or student evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school including the Data Protection Policy, Single Equality Scheme and Whole School Positive Behaviour Policy (incorporating Anti-Bullying strategies) etc.

Our procedures for video monitoring prohibits monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor suspicious behaviour and not individual characteristics.

Video monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law.

Consideration will be given to both staff and students regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment. The Headteacher will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place. The camera control will be monitored to ensure

it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas.

Cameras will be used to monitor activities around the external areas of the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, together with its visitors.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must 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 Regulation of Investigatory Power Act 2000 (RIPA).

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the surveillance scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the ICO Code of Practice have been placed at all access routes to areas covered by the school CCTV – refer to Section 8.

Information obtained through the CCTV system may only be released when authorised by the Headteacher 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.

4. Justification for Use of CCTV

4.1 Visual Recording

The Data Protection Act requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the school needs to be able to justify the obtaining and use of personal data by means of a CCTV system by conducting a Privacy Impact Assessment (PIA) – refer to the Information Commissioner's Office 'Conducting Privacy Impact Assessments' Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf . We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate and address a pressing need that we have identified. We have considered less privacy intrusive methods of achieving this need where possible. The use of CCTV to control the perimeter of the school buildings and entrances/exits for security purposes has been deemed to be justified by the Senior Leadership Team. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation and/or instances of poor behaviour, for example. CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

5. Operation of the System

- The Scheme will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed within these procedures.
- The day-to-day management will be the responsibility of both the Senior Leadership Team (SLT) during the day, out of hours and at weekends.

- The Control Room (see Section 5.1 below) will only be staffed by SLT. All cameras are monitored from a Central Control Room and are only available to the Headteacher on the secure Administrative Network.
- The CCTV system will be operated 24 hours each day, every day of the year.

5.1 Control Room

Viewing of live images on monitors in the school are usually restricted to the operator and any other authorised person where it is necessary for them to see it, eg to monitor congestion for health and safety purposes. The monitor has been positioned so that it is only visible to staff and members of the public are not allowed access to the area where staff can view them.

Recorded images are also viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy are restricted to authorised personnel.

In our school, the control room is located in the Headteacher's office as cameras show images that could not be seen by the public from the main reception and access to the CCTV control room is strictly limited to the Senior Leadership Team.

- The Headteacher will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.
- Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below.
- Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be endorsed in the Control Room log book. The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the System Manager, or his deputy and must be accompanied by him throughout the visit.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- If out of hours emergency maintenance arises, the Control Room Operators must be satisfied of the identity and purpose of contractors before allowing entry.
- A visitor's book will be maintained in the Control Room. Full details of visitors including time/date of entry and exit will be recorded.
- The Control Room is not manned out of hours and weekends so must be locked.
- During the working day when not manned the room must be kept secured.
- Other administrative functions will include maintaining video data and hard disc space, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Siting of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. The school has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV video monitoring and recording of public areas in the school may include the following:

- **Protection of school buildings and property:** The building's perimeter, entrances and exits.
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas.
- **Video Patrol of Public Areas:** Parking areas, main entrance/exit gates.
- **Criminal Investigations (carried out by the Police):** Robbery, burglary and theft surveillance.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.
- The cameras have been sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- We have checked that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

7. Covert Surveillance

The school will not engage in covert surveillance.

Certain law enforcement agencies may request to carry out covert surveillance on school premises. Such covert surveillance may require a Court Order. Accordingly, any such request made by law enforcement agencies will be requested in writing. The covert surveillance activities of public authorities are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

8. Notification – Signage

The Headteacher will provide a copy of these CCTV Procedures on request to staff, students, parents/carers and visitors to the school. These procedures describe the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use.

We must let people know when they are in an area where a surveillance system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);

- include basic contact details such as a simple website address, telephone number or email contact; and be an appropriate size.
-

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

All staff will be made aware of what to do or who to contact if a member of the public makes an enquiry about the surveillance system.

9. Storage and Retention of Recorded Images

9.1 Storage

Recorded material will be stored in a way that maintains the integrity of the information on the systems hard drive. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. Recorded material is stored in a secure environment in the Headteacher's office with a log of access kept by the Headteacher. Access to recorded material is restricted to the senior leadership team. All recorded information is secure. Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. Where encryption is not appropriate, as it may have an effect on the information that we are choosing to process, then other appropriate methods will be employed to ensure the safety and security of information. The room will be kept secure and passwords to access the system will not be disclosed.

The system will be stored in a secure environment on hard disk with automatic logs of access to the images created. Access will be restricted to authorised personnel as above. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by

other individuals in order to achieve the objectives set out above e.g. the Police, the Deputy Headteacher, the relevant Year Head, other members of the teaching staff, representatives of the DfE, representatives of the HSE and/or the parent of a recorded student. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

We will keep a record or audit trail showing how the information must be handled if it is likely to be used as evidence in court. Once there is no reason to retain the recorded information, it will be deleted. Exactly when we decide to do this will depend on the purpose for using the surveillance systems. A record or audit trail of this process will also be captured.

CCTV images are digitally recorded. It is important that our information can be used by appropriate law enforcement agencies if it's required. In this event, a copy will be made onto a removable drive and handed to the police.

9.2 Retention

The DPA does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose.

The Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. As a data controller, the School needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/ prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. Footage will be retained only within the hard drive system. It will be overwritten automatically as the disk space is used up. To account for the long summer holiday of 6 weeks, our system will retain footage for up to 8 weeks before being automatically deleted over the summer holiday period.

9.3 External drive Procedures

- In order to maintain and preserve the integrity of the Data used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
  - Each drive must be identified by a unique mark.
  - Before using, each tape/DVD must be cleaned of any previous recording.
  - The controller shall register the date and time of drive use, including drive reference.
  - A drive required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure evidence drive store. If a drive is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence drive store.
  - If the drive is archived the reference must be noted.
- Data may be viewed by the Police for the prevention and detection of crime, authorised officers of the Local Authority for supervisory purposes, authorised demonstration and training.
- A record will be maintained of the release of Data to the Police or other authorised applicants. A register will be available for this purpose.

- Viewing of Data by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.
- Should a drive be required as evidence, a copy may be released to the Police under the procedures described previously in this Code. Data will only be released to the Police on the clear understanding that the drive remains the property of the school, and both the drive and information contained on it are to be treated in accordance with his code. The school also retains the right to refuse permission for the Police to pass to any other person the tape or any part of the information contained thereon. On occasions when a Court requires the release of an original drive this will be produced from the secure evidence drive store, complete in its sealed bag.
- The Police may require the school to retain the stored Data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Headteacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request (see Section 10.2), or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9.4 Access

Drives storing the digitally captured images and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only ie the Headteacher.

10. Disclosure of Images

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (eg investigators). In relevant circumstances, CCTV footage may be disclosed:

- To the Police where the school is required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the school property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Headteacher/Manager in establishing facts in cases of unacceptable student behaviour, in which case, the parents/carers will be informed. The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the school; or
- To individuals (or their legal representatives) subject to a court order; or
- To the school's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Only the Headteacher are allowed to make external disclosures of CCTV footage.

Data will never be placed in the internet and will not be released to the media. Information may be released to the media for identification purposes but this must NOT be done by anyone other than a law enforcement agency.

Once we have disclosed information to another body, such as the police, they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

10.1 Requests by the Police

Information obtained through video monitoring will only be released when authorised by the Headteacher following consultation with the Chair of the Governing Body. If the Police request CCTV images for a specific investigation, any such request made by the Police should be made in writing.

10.2 Subject Access Requests

Staff involved in operating the surveillance system have been trained to recognise a subject access request. A log of the requests received will be kept and how they were dealt with. As mentioned in Section 9.3, each drive must be identified by a unique mark to allow easy retrieval.

On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. Where a subject access request is received for surveillance footage or other information, we are required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. This must be done by supplying them with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply.

The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort. The ICO's subject access code of practice makes clear this provision is only likely to be relevant in exceptional cases. If the data subject refuses an offer to view the footage or the data subject insists on a copy of the footage, then we must consider ways in which we can provide the data subject with this information.

We will always first attempt to provide the footage to the individual, or invite the data subject to a viewing if they consent to this.

If an individual agrees to a viewing of the footage but subsequently asks for that footage, it may be necessary, or at least good practice, to provide this footage where possible.
To exercise their right of access, a data subject must make an application in writing to the Headteacher/Manager. The school may charge up to £10 for responding to such a request and must respond to requests **within 40 calendar days** of receiving the written request and fee.

Requests for Data Subject Access should be made on an application form available from the Headteacher (refer to the school Data Protection Policy for further details).

A person should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered

to be personal data and may not be handed over by the school. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

For further information on subject access requests, refer to the ICO's 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.

10.3 Freedom of Information

The School may receive requests under the Freedom of Information Act (FOIA). We have a member of staff who is responsible for responding to freedom of information requests, and understands the school's responsibilities. We must respond within 20 working days from receipt of the request.

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

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA. Instead this request should be treated as a data protection subject access request as explained above in Section 10.2.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA.

11. Breaches of the Procedures (including security breaches)

- Any breach of these procedures by school staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action.
- Any serious breach of the procedures will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.
- Information obtained in violation of these procedures may not be used in a disciplinary proceeding against an employee of the school, or a student.

12. Monitoring and Review

Routine performance monitoring, including random operating checks, may be carried out by the Headteacher.

These procedures will be regularly reviewed, either by a designated individual within the school or by a third party. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there will be a periodic review, at least annually, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified. Refer to **Appendix B** for a sample Annual Review Checklist.

The review will take into account the following:

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include our commitment to the recommendations in the ICO Code of Practice and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provisions of the ICO Code of Practice, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

The periodic review will also ensure all information is sufficiently protected to ensure that it does not fall into the wrong hands. This will include technical, organisational and physical security. For example:

- Sufficient safeguards are in place to protect wireless transmission systems from interception.
- The ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.
- Where information is disclosed, it is safely delivered to the intended recipient e.g. by Royal Mail Special Delivery if posted or identification verified and receipt signed for if collected in person.
- The Control room and room where information is stored is secure.
- Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.
- Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.
- The process for deleting data is effective and being adhered to.
- If there been any software updates (particularly security updates) published by the equipment's manufacturer that they have been applied to the system.

13. Complaints

- Any complaints about the school's CCTV system should be addressed to the Headteacher.
- Complaints will be investigated in accordance with Section 12 of these procedures.

14. Further Information

Further information on CCTV and its use is available from the following:

- The Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
- The Information Commissioners Office (ICO) Website https://ico.org.uk/
- Information Commissioner's Office 'Conducting Privacy Impact Assessments' Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- Information Commissioner's Office 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.
- Regulation of Investigatory Powers Act (RIPA) 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents

- Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
- The School/Setting Data Protection Policy

Appendix A

Heron Hill Primary School

THE 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 Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 (Appendix 3)*

Appendix B

ANNUAL REVIEW OF CCTV SYSTEMS

This CCTV system and the images produced by it are controlled by (Insert Name) who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).
Heron Hill Primary School has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of staff and students. It will not be used for other purposes. We conduct an annual review of our use of CCTV as follows.

School/Setting:	Heron Hill Primary School	**Date:**	
Assessor:		**Signed:**	

	Satisfactory		**Problems Identified** *(if any)*	**Corrective Action Taken** *(if relevant)*	**Completed By**	**Date Complete**
	Yes	**No**				
Notification has been submitted to the Information Commissioner and the next renewal date recorded.						
There is a named individual who is responsible for the 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.						
A system has been chosen which produces clear images which the law enforcement bodies (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 the images of persons not visiting the premises.						
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).						
Information is available to help deal with queries about the operation of the system and how individuals may make access requests.						

	Satisfactory		Problems Identified *(if any)*	Corrective Action Taken *(if relevant)*	Completed By	Date Complete
	Yes	No				
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.						
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 information is restricted to appropriate staff.						
The recorded images 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 for law enforcement bodies, 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.						
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.						
Where information is disclosed, it is safely delivered to the intended recipient e.g. by Royal Mail Special Delivery if posted or identification verified and receipt signed for if collected in person.						
Staff are trained in security procedures and there are sanctions against staff who misuse 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 images.						
If there been any software updates (particularly security updates) published by the equipment's manufacturer that they have been applied to the system.						