CCTV Policy

Equalities Statement

In our Trust we work to ensure that there is equality of opportunity for all members of our community who hold a range of protected characteristics as defined by the Equality Act 2010, as well as having regard to other factors which have the potential to cause inequality, such as socio-economic factors.

Document Management	
Version Number:	V1
Date Approved:	July 2026
Next Review Date:	July 2027
Approved By:	Trust Board of Directors
Responsible For:	Company Secretary

Policy Revision Log	
Date	**Version No. Brief Detail of Change**
September 2026	V1

Contents

1. **Aims** ... 3
1.1 Statement of intent ... 3
2. Relevant Legislation and Guidance ... **4**
2.1 Legislation ... 4
2.2 Guidance ... 4
3. Other Policies/Procedures ... **4**
4. Covert Surveillance ... **4**
5. Data protection impact assessment (DPIA) ... **4**
6. Contact Us ... **5**
7. Complaints ... **5**
Appendix 1 - Location of the Cameras ... **6**
A1.1 - The Use of CCTV in Private Areas ... 6
Appendix 2 - Roles and Responsibilities ... **7**
A2.1 The Chief Executive Officer ... 7
A2.2 The Headteacher ... 7
A2.3 The Data Protection Officer (DPO) ... 7
A2.4 The School Data Protection Lead (DPL) ... 7
A2.5 The System Manager ... 8
Appendix 3 - Operation of the CCTV System, and Storage of/Access to Footage ... **9**
A3.1. Operation of the CCTV System ... 9
A3.2. Storage of CCTV Footage ... 9
A3.3. Access to CCTV Footage ... 9
A3.4 Staff Access ... 9
A3.5 Subject access requests (SAR) ... 10
A3.6 Third-party access ... 10
Appendix 4 - Security The system manager will be responsible for overseeing the security of the CCTV system and footage ... **11**
Appendix 5 - ICO CCTV Checklist ... **12**
Appendix 6 - CCTV Access Log ... **13**

1. Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings
- To assist in the monitoring of the wellbeing of animals
- To be able to identify the number plate of a vehicle that enters or exits the premises
- Evidence of delivery of goods
- Monitor premises entry points

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and the UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant Legislation and Guidance

This policy is based on:

2.1 Legislation

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

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

3. Other Policies/Procedures

- Data Protection Policy
- Privacy Notices
- Safeguarding policy
- Protection of Biometric Data Policy
- Records Retention Schedule

4. Covert Surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

5. Data protection impact assessment (DPIA)

The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in Section 1.1).

When the CCTV system is replaced, developed or upgraded, and/or whenever cameras are moved or additional cameras are installed, a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA. If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

6. Contact Us

If you have any questions, concerns or would like more information about anything mentioned in this policy, please contact the Company Secretary in the first instance:

- enquiries@swale.at

Our DPO service is provided by:
Invicta Law Ltd, 1 Abbey Wood Road, Kings Hill, West Malling, Kent, ME19 4YT

- dpo@invicta.law

If you require any Estates support relating to anything mentioned in this policy, please contact Estates in the first instance:

- estates@swale.at

If you require any IT support relating to anything mentioned in this policy, please contact IT using the IT Helpdesk ticket system.

7. Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or you have any other concern about our data processing, we encourage you to raise this with us in the first instance by completing this Google Form (https://forms.gle/2EEVPyBTRjyDwy4t6)

Alternatively you can email our Data Protection Officer (details at Point 6). You also have the right to make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Appendix 1 - Location of the Cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in Section 1.1).

For details on where CCTV cameras are located, please see below (pages 7-9)

Wherever cameras are installed, appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

Cameras are not, and will not be, intentionally directed toward public spaces or private property outside of the school grounds. However, it is recognised that cameras positioned to monitor site entrances may capture incidental 'overspill' of areas immediately adjacent to the school perimeter.

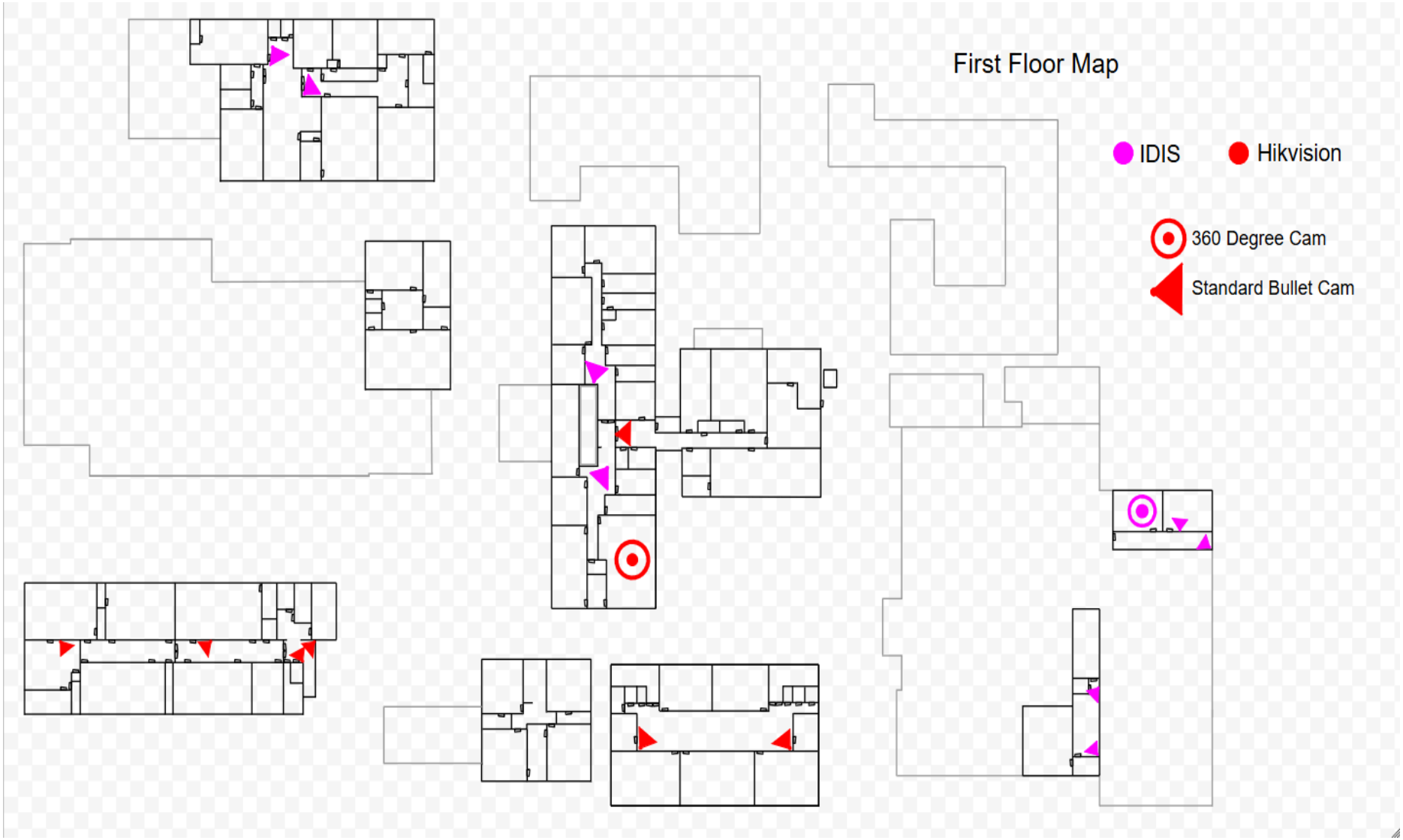
Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

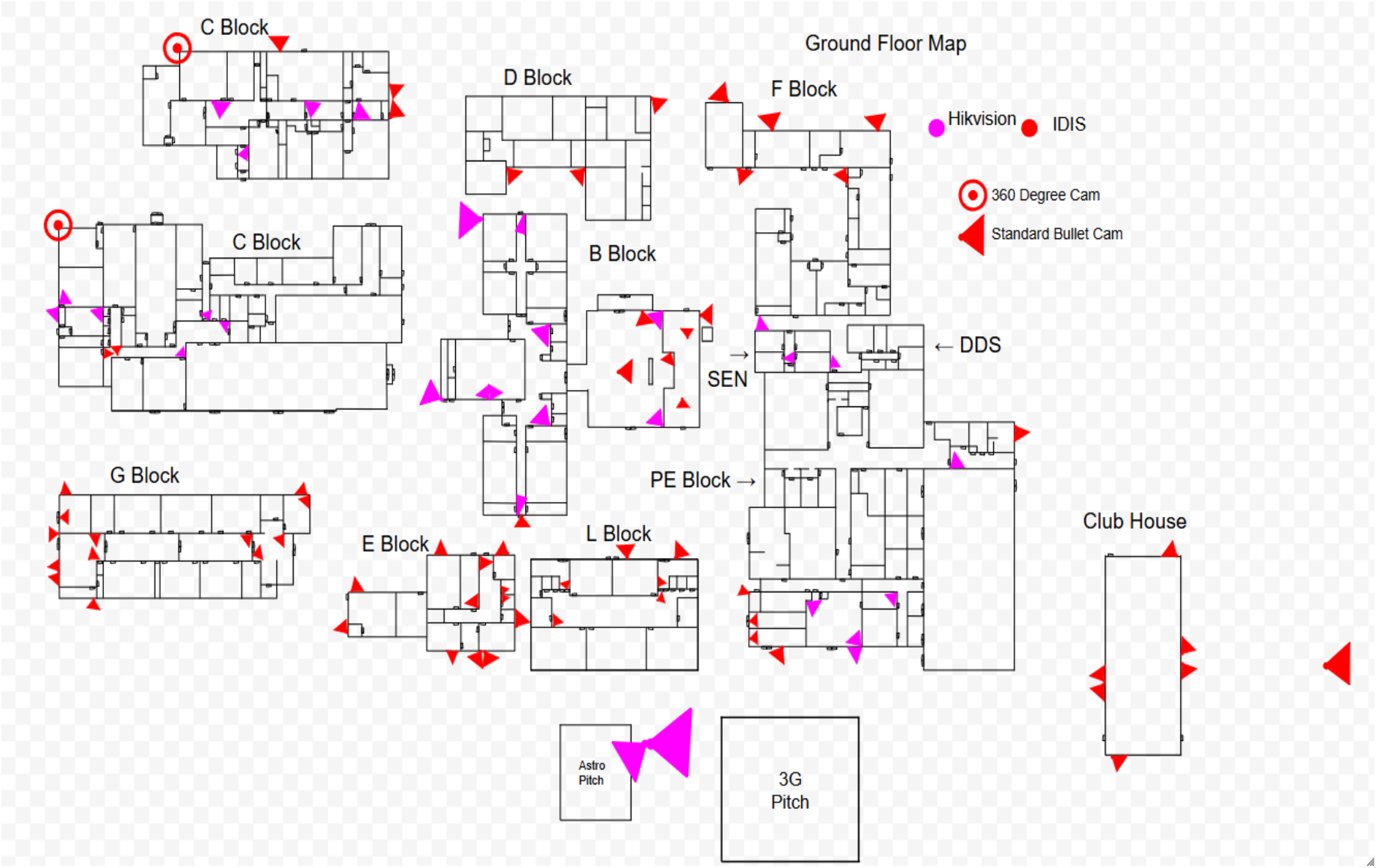
A1.1 - The Use of CCTV in Private Areas

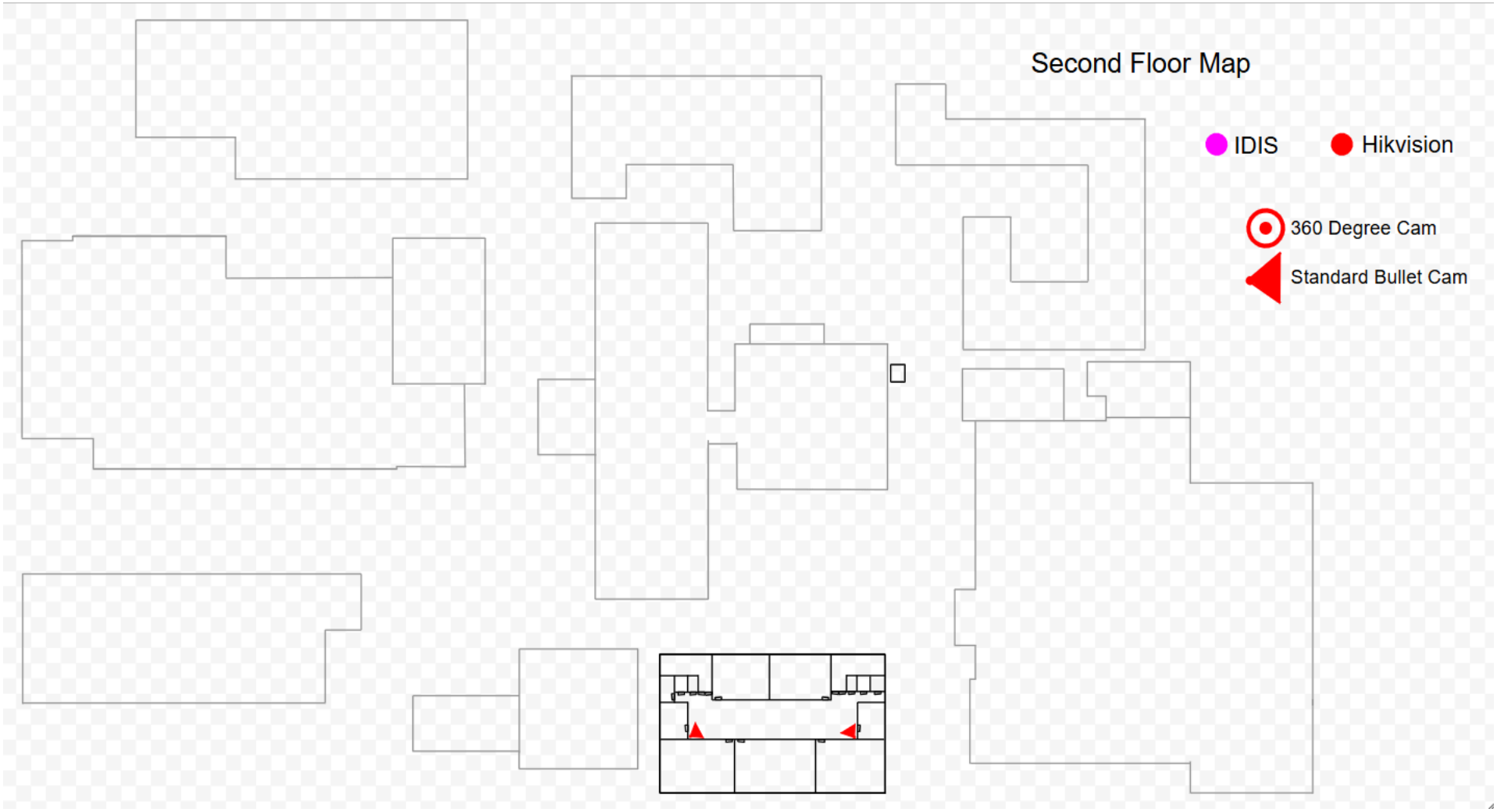
The use of CCTV in toilets and changing rooms is not considered fair or proportionate by the ICO apart from in exceptional cases, such as dealing with repeated serious antisocial behaviour, when it may be necessary to have surveillance in private areas. The threshold for using CCTV in these locations is extremely high, and the ICO's position is clear that schools must trial less intrusive methods first to tackle the original purpose of the surveillance. These alternative methods may include:

- Increased staff presence in these areas
- Pupil toilet passes
- Limited number of students in the area at one time

Schools are required to keep a formal record of the findings from these trials to demonstrate their necessity. Additionally, a consultation with key stakeholders is highly encouraged to maintain transparency and trust. Prior to any installation, a full Data Protection Impact Assessment (DPIA) must be completed and the purpose must be continually reviewed for necessity and proportionality to ensure the privacy of the individuals involved is protected.


First Floor Map
IDIS
Hikvision
360 Degree Cam
Standard Bullet Cam


Ground Floor Map
C Block
C Block
D Block
B Block
F Block
Hikvision
IDIS
360 Degree Cam
Standard Bullet Cam
← DDS
SEN →
PE Block →
G Block
E Block
L Block
Club House
Astro Pitch
3G Pitch


Second Floor Map
IDIS
Hikvision
360 Degree Cam
Standard Bullet Cam

Appendix 2 - Roles and Responsibilities

A2.1 The Chief Executive Officer

The Chief Executive Officer has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in Section 2.1) is complied with.

A2.2 The Headteacher

The Headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system;
- Liaise with the Data Protection Officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified;
- Ensure that the guidance set out in this policy is followed by all staff;
- Ensure the the CCTV Policy is completed and up to date to maintain the school's compliance with legislation;
- Ensure that a DPIA has been completed for any CCTV system currently installed at the school, which is to be updated when additional cameras are deployed;
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and in data protection;
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and having taken into account the result of a Data Protection Impact Assessment;
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.

A2.3 The Data Protection Officer (DPO)

The DPO will:

- Advise on Subject Access Requests in line with the UK GDPR and Data Protection Act 2018;
- Monitor compliance with UK data protection law;
- Advise on and assist the school with carrying out Data Protection Impact Assessments;
- Act as a point of contact for communications from the Information Commissioner's Office (ICO);

A2.4 The School Data Protection Lead (DPL)

The School DPL will:

- Ensure those with authorisation to access the CCTV system and footage have received appropriate training in the use of the system and in data protection;
- Train all staff to recognise a subject access request;
- Deal with Subject Access Requests in line with the UK GDPR and Data Protection Act 2018;
- Assist with carrying out Data Protection Impact Assessments;
- Ensure data is handled in accordance with data protection legislation;
- Ensure footage is obtained in a legal, fair and transparent manner;
- Ensure footage is destroyed when it falls out of the retention period;
- Liaise with Estates and IT to ensure that the CCTV systems are working properly and identify any future upgrades that may be required (e.g to ensure the footage they produce is of high quality so that individuals pictured in the footage can be identified);
- Liaise with IT to ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces;
- Liaise with Estates and IT to ensure that new or replacement CCTV cameras are to current SAT specification and connect to existing systems or form a platform for all future cameras;

- Liaise with IT to ensure that the CCTV system(s) are supported and meet the DfE requirements on software;
- Carry out seasonal-termly checks to determine whether footage is being stored accurately, and being deleted after the retention period;
- Receive, consider and log requests for third-party access to CCTV footage;

A2.5 The System Manager

The System Manager (School Site Manager) will:

- Take care of the day-to-day maintenance and operation of the CCTV system;
- Check the system for faults and security flaws termly;
- Ensure the data and time stamps are accurate termly.

Appendix 3 - Operation of the CCTV System, and Storage of/Access to Footage

A3.1. Operation of the CCTV System

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system will not record audio.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

A3.2. Storage of CCTV Footage

Footage must be a minimum of 1080p and 15 frames per second. 25 frames per second should be used in high risk areas, requiring facial recognition or fast moving objects such as vehicles.

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

The DPL will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period.

A3.3. Access to CCTV Footage

Access must be kept to an absolute minimum.

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in Section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log (see Appendix 6).

Access must only be while on school site, and remote access to CCTV will not be provided.

Any visual display monitors must be positioned so only authorised personnel are able to see the footage.

A3.4 Staff Access

The following members of staff have authorisation to access the CCTV footage:

- The Headteacher: Nick Smith
- Senior Leaders: Alex Campbell (DHT), Sarah Webb (SAHT) , Orla Wheeler (SAHT), Chris Collins (AHT) and Derrick Hutley-Anderson (AHT)
- Associate Head of Sixth Form: Matt Judd
- The DPL: Sarah Scott-Drysdale
- The system manager: Matthew Thrower
- Site Manager: Mark Cork

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

A3.5 Subject access requests (SAR)

According to the UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving SAR the school will immediately issue a receipt and will then respond within 1 calendar month.

All staff have received training to recognise SARs. When a SAR is received, staff should inform the DPL in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school must conceal their identities by blurring out sections of video, reducing the timeframe of the footage or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with a SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Footage transfers must be conducted via the "office external" Google account (your IT support will provide you with a link) to a specific, named recipient for a limited duration; files must be encrypted, with the password provided through a separate communication channel. This excludes transfers to secure police force email addresses which are acceptable without the additional security protocols.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

A3.6 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in Section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the Headteacher and the DPL.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with the UK GDPR.

All disclosures will be recorded by the DPL.

Appendix 4 - Security **The system manager will be responsible for overseeing the security of the CCTV system and footage**

- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

Appendix 5 - ICO CCTV Checklist

We, [school name] have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

Check	Detail	Date
Our system is processing footage of identifiable individuals and is processing personal data. We have registered as a controller and submitted a relevant data protection fee to the Information Commissioner's Office (ICO). We have also recorded the next renewal date.	Confirm here	
There is a named individual who is responsible for the operation of the system.	Enter name here	
Prior to processing we have clearly defined the problem we are trying to address. We regularly review our decision to use a surveillance system.	Confirm here	
We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018.	Insert link to DPIA here	
Our system produces clear images which we can easily disclose to authorised third parties. For example when law enforcement bodies (usually the police) require access to investigate a crime.	Confirm here	
We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.	Confirm here	
There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system.	Confirm here	
We securely store images from this system for a defined period and only a limited number of authorised individuals may have access to them.	Define the period here Name the authorised individuals here	
We know how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted.	Confirm here	

Signed: _____ Print Name: _____

Appendix 6 - CCTV Access Log

Access to CCTV recordings will only be given to authorised persons, for the purpose of pursuing the aims stated in Section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record the following details in the access log:

- Date of Access;
- Date of Footage;
- Time (Start/End);
- Accessing Person (Name and Job Title);
- Purpose of Access;
- Footage Details (Camera # / Location);
- Data subjects;
- Action Taken (Viewed, Exported, Deleted etc);
- Authorised By (Manager Initials).

A template Access Log template can be found below - *the school must make a copy for its own records*.

CCTV Access Log Template