CCTV Policy

Policy reviewed and updated	March 2025
Date of next review	March 2026
This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation where appropriate	

Contents:

Statement of intent

At Harefield School, we take our responsibility towards the safety of staff, visitors and students very seriously, including the security and integrity of the building. To that end, we use surveillance cameras to monitor any instances of aggression, anti-social behaviour or physical damage to our school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with data protection legislation, including General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018
- The images that are captured are useable for the purposes for which we require them
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Maintain a safe environment
- Ensure the welfare of students, staff and visitors
- Deter criminal acts against persons and property
- Assist the police in identifying persons who have committed an offence

1.Legal framework

1.1 This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (GDPR) as applied in the Data protection Act 2018
- The Freedom of Information Act 2000
- 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

1.2 This policy has been created with regard to the following statutory and non- statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

1.3 This policy operates in conjunction with the following school policies:

- ICT Policy
- Data Protection Policy (GDPR compliant)
- Safeguarding Policy
- Behaviour for Learning Policy

2. Definitions

2.1 For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video or live footage. For the purpose of this policy only video footage will be applicable.
- **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

2.2 Harefield School does not condone the use of covert surveillance when monitoring the school's staff, students and/or visitors and other site users.

2.3. Any overt surveillance will be clearly signposted around the school.

3. Roles and responsibilities

3.1**.** The role of the Data Protection Officer (DPO)/Data Lead includes:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's privacy impact assessment (PIA), and under the GDPR the data protection impact assessment (DPIA), and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.

3.2. Harefield School, as the corporate body, is the data controller. The governing board of Harefield School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The Data Lead deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

3.4. The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for

longer than is necessary.
- Protecting footage containing personal data against accidental or unlawful destruction, alteration and disclosure – especially when processing over networks

3.5 The role of SLT includes:

- Meeting with the IT Manager/Data Lead to decide where CCTV is needed to justify its means
- Conferring with the IT Manager/Data Lead with regard to the lawful processing of the surveillance and CCTV footage
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully
- Communicating any changes to legislation with all members of staff

4. Purpose and justification

4.1. The school will only use surveillance cameras for the safety and security of the school and its staff, students and visitors.

4.2. Surveillance will be used as a deterrent for violent behaviour, theft and criminal damage to the school.

4.3. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any changing facility.

5. The data protection principles

5.1. Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Objectives

6.1 The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of students, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

7. Protocols

7.1 The surveillance system will be registered with the ICO in line with data protection legislation.

7.2 The surveillance system is a closed digital system which does not record audio

7.3 Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice

7.4.The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

7.5.The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

8.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

8.2. The school's authorised CCTV system operators are:

a. Jared Martin
b. Trevor Chidgey
c. Amit Tailor
d. Salma Riley

The following staff have permission to view footage but not share\give access:

a. Trudy White
b. Karen Raper
c. Ria Booker
d. Nicola Sweeney
e. Ryan Bourne

f. George Fellows

The following staff have permission to view footage and authorise access:

a. Salma Riley
b. Helen Timmins
c. Steven Fish
d. Farah Ahmed
e. Helen Howley
f. Natalie Jellis
g. Sonia Ral
h. Neeta Ghedia
i. Helen Howley

8.3. The main control facility is kept secure and locked when not in use.

8.4. Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.

8.5. Surveillance and CCTV systems will not be intrusive.

8.6. Any unnecessary footage captured will be securely deleted from the school system.

8.7 Any cameras that present faults will be repaired ASAP to avoid any risk of a data breach.system.

8.8. The CCTV system can be accessed from the ICT office, Site Team offices and Headteachers office computers.

9. Privacy by design

9.1. The use of surveillance cameras and CCTV will be critically analysed using a PIA (Privacy Impact Assessment) – under the GDPR this will become a DPIA (Data Protection Impact Assessment) but it will follow the same principles of a PIA

9.2. A DPIA will be reviewed prior to the installation of any additional surveillance and CCTV system equipment.

9.3. If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions

9.4. The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

10. Code of practice

10.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles

10.2. The school notifies all students, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds and main building where cameras are based.

10.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose

10.4. All surveillance footage will be stored for 28 days for security purposes; the IT manager is responsible for keeping the records secure and allowing access.

10.5. The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors**.**

10.6. The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, students and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

10.7. The surveillance and CCTV system will:

a. Be designed to take into account its effect on individuals and their privacy and personal data.
b. Have clear responsibility and accountability procedures for images and information collected, held and used.
c. Have defined policies and procedures in place which are communicated throughout the school.
d. Only keep images and information for as long as required.
e. Restrict access to retained images and information with clear rules on who can gain access.
f. Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
g. Be subject to stringent security measures to safeguard against unauthorised access.
h. Be regularly reviewed and audited to ensure that policies and standards are maintained.
i. Only be used for the purposes for which it is intended, including supporting public safety, the protection of students, staff and volunteers, and law enforcement.

10.8. Be accurate and well maintained to ensure information is up-to-date.

11. Access

11.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. Indivuals have the right to submit a SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.3. The school will verify the identity of the person making the request before any information is supplied.

11.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.5. Where an SAR (Subject Access Request) has been made electronically, the information will be provided in a commonly used electronic format**.**

11.6.Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher and Designated Safeguarding Lead, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.7.Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.8. All fees will be based on the administrative cost of providing the information.

11.9. All requests will be responded to without delay and at the latest, within one month of receipt.

11.10. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.11. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal

11.12. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

11.13. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

11.14. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

a. The police – where the images recorded would assist in a specific criminal inquiry
b. Prosecution agencies – such as the Crown Prosecution Service (CPS)

c. Relevant legal representatives – such as lawyers and barristers
d. Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

11.15. Requests for access or disclosure will be recorded and the Headteacher and DPO will make the final decision as to whether recorded images may be released to persons other than the police.

12.Monitoring and review

12.1 This policy will be monitored and reviewed on an annual basis, or in light of any changes to relevant legislation by the DPO and the Headteacher.

12.2. The Headteacher and DPO will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly**.**

12.3. The scheduled review date for this policy is annually.

APPENDIX A: CCTV SUBJECT ACCESS REQUEST FORM

Under the terms of the Data Protection Act 2018 an individual has the right to request a copy of any personal information held about them by Harefield School, whether it is in hard copy, electronic, or CCTV. Should you wish to exercise your right in requesting disclosure of your data recorded on CCTV please complete this form, providing as much information as possible.

Please note that any request by a third party to view CCTV images must be approved by the Data Protection Officer, who will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. Images will be provided within 30 calendar days of receiving a request.

<table>
<tr><th colspan="2">1. PERSONAL DETAILS</th></tr>
<tr><td colspan="2">Applicant's full name:</td></tr>
<tr><td colspan="2">Applicant's postal address:</td></tr>
<tr><td colspan="2">Applicant's email address:</td></tr>
<tr><th colspan="2">2. INFORMATION REQUIRED</th></tr>
<tr><td colspan="2">To help us find the CCTV data you require, please complete the following section.</td></tr>
<tr><td colspan="2">Location/position of CCTV camera:</td></tr>
<tr><td>Date image taken:</td><td>Time image taken:</td></tr>
<tr><td colspan="2">Brief description of the applicant's appearance and likely activities captured by CCTV:
(A recent photograph may also be required to assist identification of the relevant images.)</td></tr>
</table>

Please give any other information that might assist us in finding the information required:		
Do you require a hard copy of the image or would “viewing” the images be sufficient?	Hard copy ☐	Viewing ☐

3. DECLARATION

Delete as applicable.

□ I confirm that all of the information I have provided is correct and that I am the Data Subject.

□ I confirm that I am acting on behalf of the Data Subject and have attached proof of my authority to do so.

Name:	
Postal address:	
Email address:	
Signed:	Date:

4. PROOF OF IDENTITY

If you are applying on someone else’s behalf, please attach documented authority to act on the data subject’s behalf.

5. SUBMITTING A REQUEST

After completing the application form, please check to ensure that all the information you have provided is accurate and all the required documents and the fee are attached.

Please return the application form to the Data Protection Officer.

APPENDIX B: CCTV POLICE ACCESS REQUEST AND RECORDING REGISTER

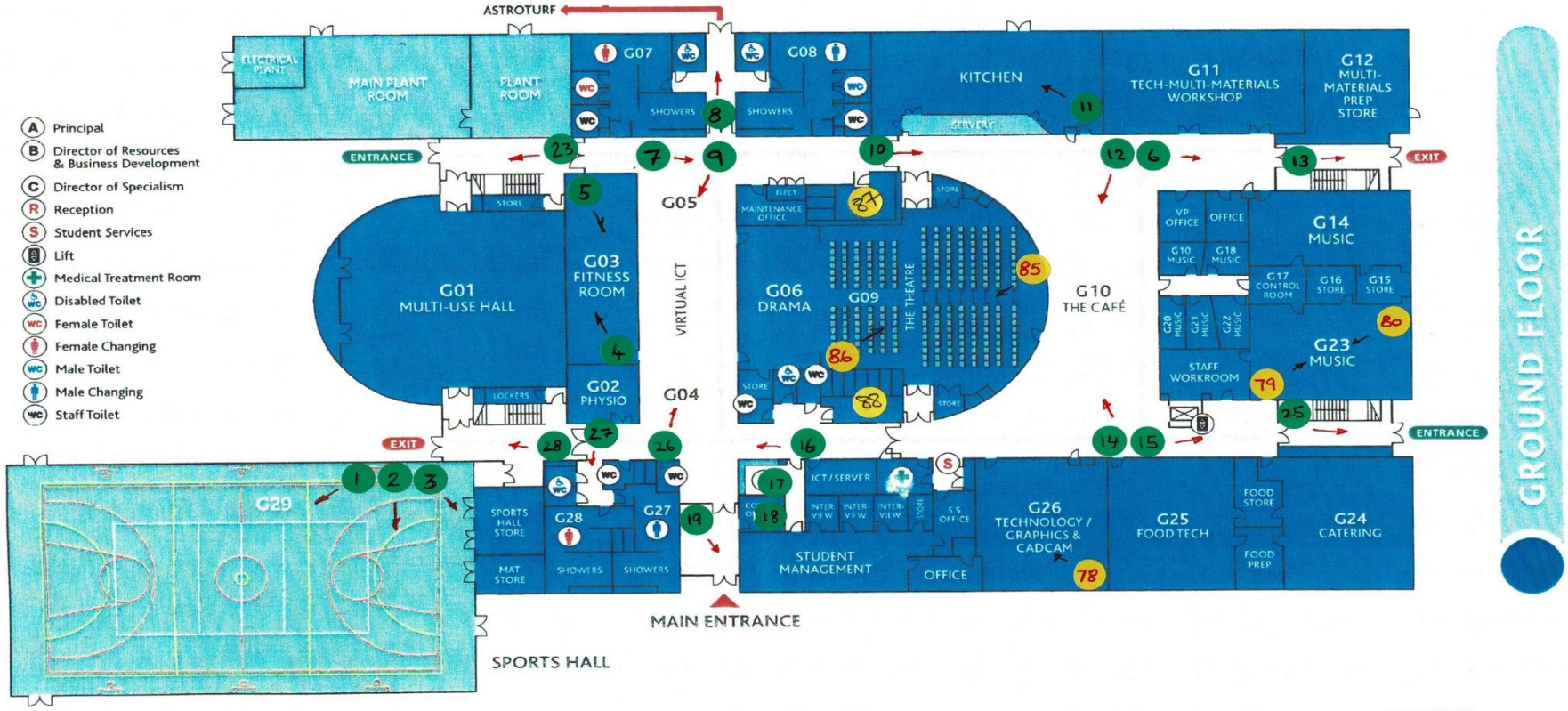
Data Protection Act 2018

Description of Incident / Person(s) involved:	**Camera Location:**	
Date of incident:	**Approximate time of incident (24 hours):**	
Name of person who requested to view the recorded image:	**Signature:**	**Date of request:**
Contact Telephone Number:	**Email:**	
Name of person who recorded the image(s) onto disc:	**Signature:**	
Date images were recorded:	**Disc reference number:**	
Name of person who received the image(s):	**Signature:**	**Date received:**
Name of person who received the image(s):	**Signature:**	**Date received:**

APPENDIX C: CCTV DISC BURNING LOG

Date	Reason Needed	Name	Date Copied	Date Destroyed	Signature 1	Signature 2 (IT manager)

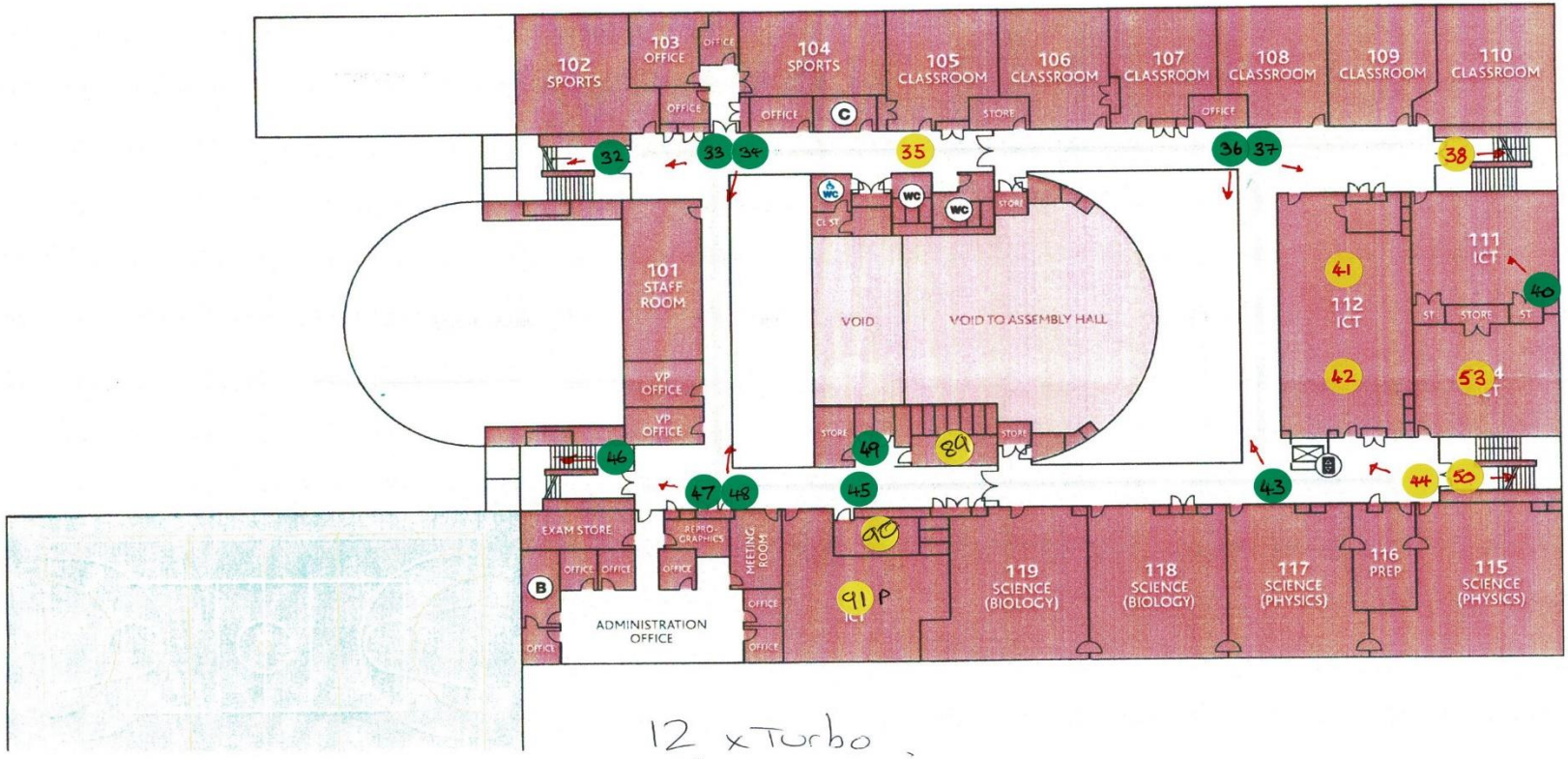
APPENDIX C: CCTV SITE PLANS



24 x Turbo.
7 x IP STATIC

DESIGNED BY:

SCHOOLWATCH
CCTV FOR SCHOOLS & COLLEGES



12 x Turbo
5 ~~8~~ x IP Static
4 ~~8~~ x 6mp 360.
1 x 180

DESIGNED BY:

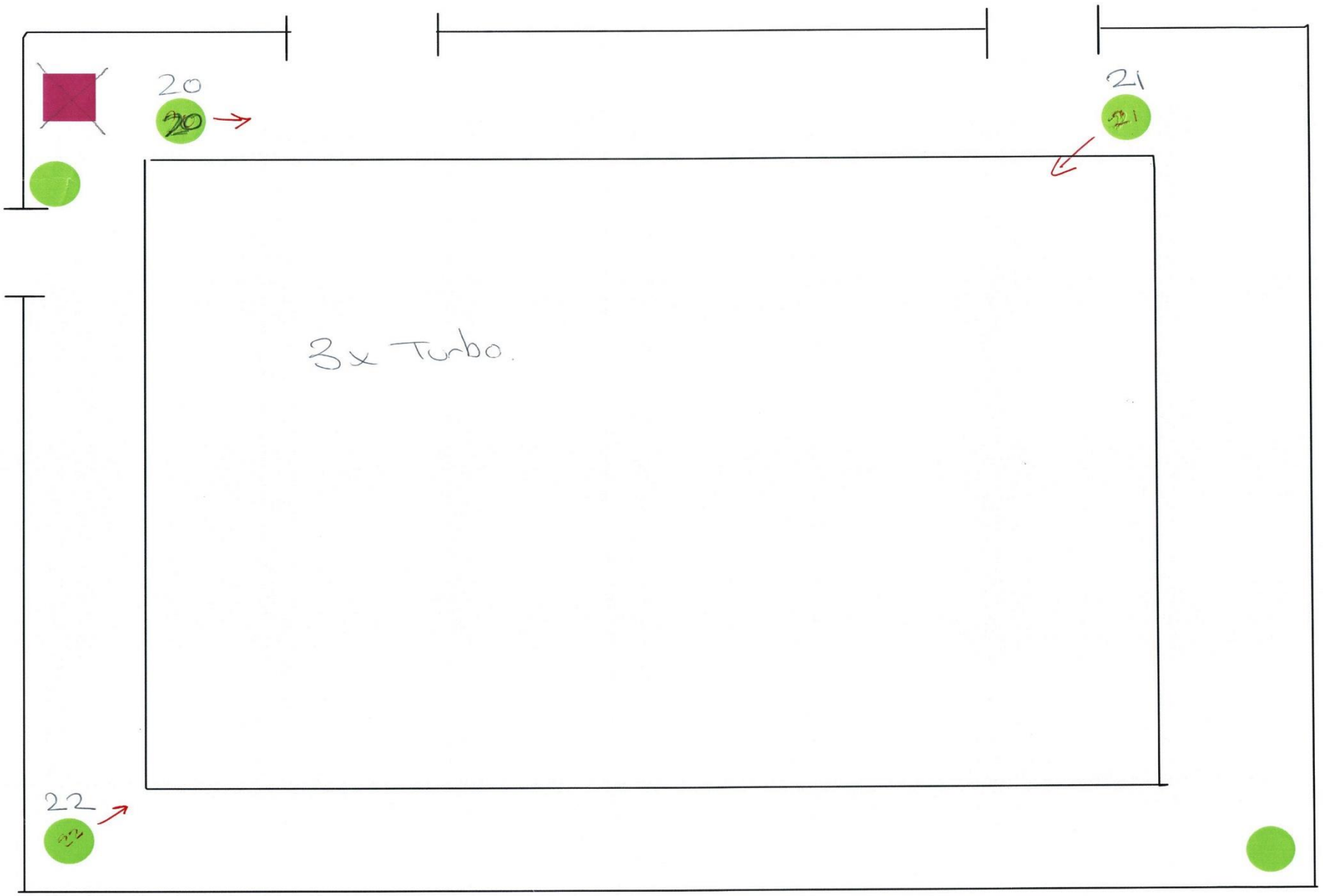
SCHOOLWATCH
CCTV FOR SCHOOLS & COLLEGES

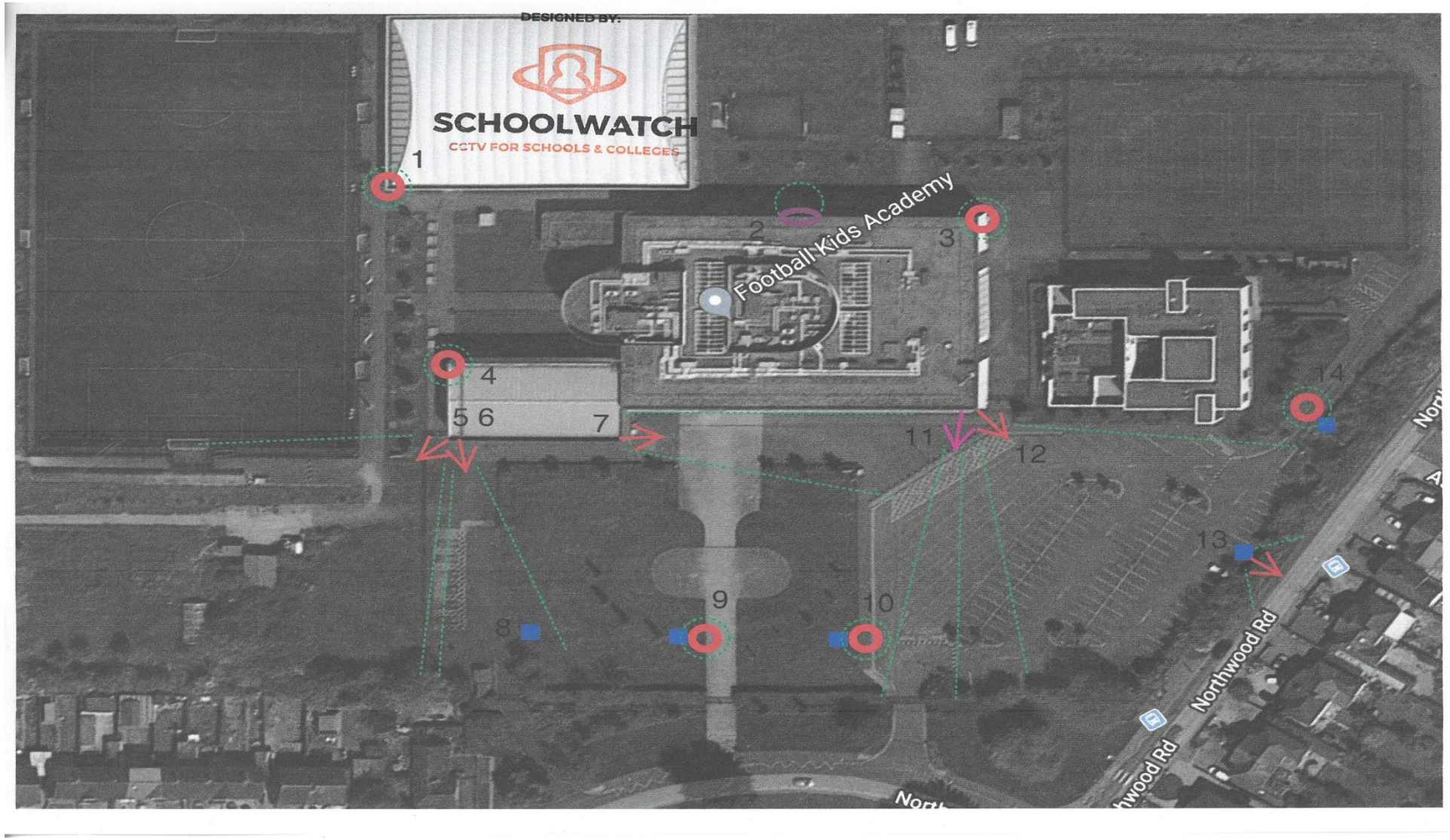
The Harefield Academy

18 x Turbo
6 ~~6~~ x Static IP.
3 x 360.

DESIGNED BY:

SCHOOLWATCH
CCTV FOR SCHOOLS & COLLEGES


20
21
3x Turbo
22


DESIGNED BY:
SCHOOLWATCH
CCTV FOR SCHOOLS & COLLEGES
Football Kids Academy
1
2
3
4
5 6
7
8
9
10
11
12
13
14
Northwood Rd