



THE VYNE COMMUNITY SCHOOL

CCTV POLICY

Updated: November 2025
Next Review: November 2026

Linked Policies

- **Acceptable Behaviour of Visitors Policy**
- **Data Protection Policy**
- **Freedom of Information Policy**
- **Privacy Notices**

Contents

1. Introduction
2. Purposes of the CCTV Scheme
3. The guiding principles of the Surveillance Camera Code of Practice
4. Details about the CCTV system
5. Operation of the CCTV system (including location)
6. Signs and privacy notices
7. Storage and Retention
8. Staff training
9. Requests for CCTV footage
10. Review
11. Complaints and concerns
12. Related policies and procedures
13. Other sources of information

1. Introduction

This policy is to regulate the management, operation and use of the CCTV scheme at The Vyne School.

2. Purposes of the CCTV Scheme

The school's use of CCTV must only be for specified purposes which are in the pursuit of legitimate aims and are necessary to meet an identified pressing need. The specified purposes for the school's use of CCTV are:

- To protect the school buildings, grounds and their assets.
- To increase personal safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime.
- To assist in identifying , apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the School and act as a deterrent for violent or destructive behaviour
- To assist with traffic management on site

3. The guiding principles of the Surveillance Camera Code of Practice

The school adopts the guiding principles in the Surveillance Camera Code of Practice which are as follows:

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 user 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

In addition, the school will ensure that its use of CCTV complies with data protection legislation (including the UK GDPR and the Data Protection Act 2018).

4. Details about the CCTV system

- The system comprises both fixed and dome cameras located around the school site.
- The CCTV system will operate 24 hours each day, every day of the year.
- Audio is disabled on all devices thus sound is not recorded.
- The Network Manager and Site Manager will be responsible for the day to day operation of the system.
- The school's Data Protection Officer will be responsible for monitoring compliance with this policy.
- A data protection impact assessment will be carried out prior to installation of significant additional CCTV system equipment
- CCTV systems of the School have been notified to the Information Commissioner, Registration Number Z5875703

5. Operation of the CCTV system (including location)

The Governing Finance and Resources Committee has considered the proper location of CCTV cameras, where they exist, in and around the school. The location of cameras are based upon a variety of information including security, health and safety. Cameras are restricted to only monitor areas required under the scheme.

- The system used produces clear images and these images can be taken from the system when required by authorised users.
- The cameras have been sited to provide clear images
- The cameras have been positioned to avoid capturing the images of persons not visiting the school and to monitor those spaces intended to be covered by the policy.
- Cameras will not be positioned in areas where there is a particularly high expectation of privacy however, cameras are positioned over wash basins of toilet areas for the purposes of reducing graffiti, vandalism, vaping/smoking. Real time monitoring is not in place; however a feed is visible to the Site Manager as part of ensuring the system remains operational. Footage is only viewed in light of an incident and can only be viewed by authorised personnel.
- Recorded material will be stored in a way that maintains the integrity of images.
- Regular checks are carried out to ensure that the system is working properly, producing high quality images and is showing the correct time. Checks should be made that data is being deleted at the end of the retention period.
- Viewing of any live monitors must be restricted to the operator. Viewing of recorded images should take place in a restricted area to which only authorised staff have access to.
- The images from the CCTV system are securely stored where only a limited number of authorised persons may have access to them
- Where cameras store data, the data stored will be encrypted in order to prevent viewing should any unauthorised removal/theft occur.
- When installing cameras consideration must be given to the physical conditions in which the cameras are located.
- The Site Manager will ensure that cameras will be properly maintained, and ensure that any damaged/non-working camera is fixed within a specific time period.
- The main control facility is kept secure and locked when not in use.

6. Signs and privacy notices

Individuals have the right to be informed about the use of their data including any CCTV images of them.

- The school will ensure that where cameras are in use clear signage is put in place so that members of the public and staff are aware that they are entering an area that is monitored by cameras.
- The school will ensure that the signs are clearly visible and will review regularly

The school's privacy notice which covers its use of CCTV can be found on the school website.

7. Storage and Retention

- The school will retain the data for no longer than 31 days (except where it is necessary to retain specific data for longer for example for the purposes of an ongoing investigation).
- The data will be stored securely at all times, and in line with the retention period.
- The data will be erased permanently and securely at the end of the retention period.
- Images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.

8. Staff training

Staff using camera systems will have appropriate training. Staff will be trained in their responsibilities under this policy and related policies and procedures and should be aware of the security and disclosure procedures for the scheme and the rights of individuals regarding their recorded images.

9. Requests for CCTV footage

(a) Data subject requests (SAR)

Individuals have certain legal rights in respect of their personal data including their CCTV images. The rights that will be most relevant to CCTV use will be:

- **Right of access** (i.e. data subject wishes to access their CCTV images)
- **Right to object** (i.e. data subject objects to the use of CCTV capturing their image)
- **Right to be forgotten** (i.e. data subject wishes to have their CCTV footage erased)

Any data subject requests in respect of CCTV footage, will be dealt with in accordance with the school's data subject requests process details of which can be found in the Privacy Notices on our website. It should be noted that if the data contains third parties, this may be difficult to redact and therefore may be exempt from disclosure.

1. All disks containing images belong to, and remain the property of, the school.
2. The SAR should contain information to help the school verify the identity of the person making the request eg
 - A specific date and time
 - Proof of identity
 - A description of themselves
 - Up to date contact details

before any information is supplied (the 30 days commences from the date proof of ID is received).

3. 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.

4. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.
5. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
7. All fees will be based on the administrative cost of providing the information.
8. All requests will be responded to without delay and at the latest, within one month of receipt.
9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months.
10. 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. 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.
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.
13. The School may refuse to share the footage if:
 - Other people can be seen in it
 - It is not possible to edit out other people to protect their identity
 - It may put an ongoing criminal investigation at risk
14. The School may invite the Subject to a viewing of the footage, by prior agreement if it is not possible to provide the footage

(b) Freedom of Information requests

As the school is a public authority for the purposes of the Freedom of Information Act 2000 it may receive FOI requests for CCTV footage. The school will deal with any FOI requests concerning CCTV in accordance with its FOI procedure

(c) Internal access

- All staff should be aware of the restrictions set out in this policy in relation to access to, and disclosure of, recorded images.
- Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment. This is to ensure the rights of individuals are preserved and to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
- All access to the medium to which images are recorded will be documented.
 - Date and time, reason for request, by whom, outcome
- If images are removed and retained for evidential purposes this will be documented.

(d) External requests

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

- The police - where images recorded would assist a specific criminal inquiry
- Prosecution agencies - such as the Crown Prosecution Service (CPS)
- Relevant legal representatives - such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the FOI

i. All requests for access or for disclosure will be recorded, if access or disclosure is denied, the reason will be documented.

ii. If access to or disclosure of the images is allowed, then the following will be documented:

- Date and time at which access was allowed or date the disclosure was made.
of removal
- The identification of any third party who was allowed access or to whom disclosure was made.
- The reason for allowing access or disclosure.
- Location of the images.
- Any crime incident number to which images may be relevant.
- Signature of person authorised to collect the medium - where appropriate
- Recorded images will not be made more widely available for example- they should not be routinely made available to the media or placed on the internet.
- The decision to make footage more widely available rests with the Headteacher and the reason for that decision documented
- If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.
- The School Business Manager will periodically monitor records of system access.

Review

The school's use of CCTV will be reviewed annually, or in light of any changes to relevant legislation by the DPO.

This policy shall be reviewed annually and updated as required.

10. Complaints and concerns

Any complaints or concerns about the school's use of CCTV should be sent to the Data Protection Officer via enquiries@vyne.hants.sch.uk