PONTARDDULAIS COMPREHENSIVE SCHOOL
YSGOL GYFUN PONTARDDULAIS

CCTV Policy and Guidelines

Mr. G. Rees

Headteacher

Mrs. S. Bradshaw

Chair of Governors

Review Date: 2024
Next Review Date: 2027

Learn to live... live to learn | Byw I ddysgu... dysgu byw

1. Introduction

Closed Circuit Television (CCTV) can be a valuable resource in surveillance and security and is widely used by local authorities in a range of premises and situations. However, because of the potentially sensitive nature of surveillance, there are codes, guidelines and legislation which must be complied with in order to operate a CCTV scheme legally and fairly.

Images and audio recorded by a CCTV scheme are deemed to be personal data under the terms of the General Data Protection Regulation ('the GDPR') and the Data Protection Act 2018 ('the DPA'). The GDPR defines 'personal data', as any data relating to living individuals from which they can be identified, either directly from the data itself or by another individual when combined with other data that is in, or likely to come into, their possession.

Personal data is not therefore limited to the ability to name an individual. If images of an individual's features are processed and an individual can then be identified from those images, this will by extension constitute personal data.

Data is considered to have been processed from the point at which it is recorded and retained, even if the data is not subsequently viewed by anyone.

As with their other personal data, the records from a CCTV scheme may be requested by members of the public in the form of a Subject Access Request within the terms of the GDPR and DPA.

2. Scope of the policy

This policy and supporting guidance explains and confirms how Pontarddulais Comprehensive School ("the School") manages its CCTV systems, determines who has access to the CCTV data processed by those systems and under what circumstances, including the procedures that will be followed in regard to providing rights of access.

This document must be read in conjunction with the *CCTV Code of Practice* (revised edition 2017), issued by the Information Commissioner's Office (ICO), the *Surveillance Camera Code of Practice pursuant to Section 29 of the Protection of Freedoms Act 2012* ("SC Code") issued by the Home Office, and the Council's Data Protection Policy.

This policy forms part of a suite of policies relating to data protection which outline the School's public responsibilities in this regard. The use of CCTV footage for the purposes of monitoring or disciplining staff is covered by a separate Human Resources policy.

.

3. Purpose of the policy

This policy identifies the procedures and processes to be followed by the School when planning, implementing and operating a CCTV scheme on School premises. It is important that this Policy is read by those considering the installation of a CCTV scheme, and that its contents are complied with following implementation.

CCTV schemes must be compliant with the above-mentioned codes of practice (see section 2), the GDPR and the DPA. This public policy also outlines how the School will meet its obligations and administer the citizen rights contained within this legislation.

All enquiries about and proposals for new CCTV installations must in the first instance be directed to the School's Data Protection Officer, who may require a Data Protection Impact Assessment to be completed.

4. Legislation affecting the policy

Any CCTV Scheme owned and operated by the School must comply with the following legislation:

- The GDPR and DPA;
- The Human Rights Act 1998;
- The Protection of Freedoms Act 2012;
- The Freedom of Information Act 2000;
- The Regulatory and Investigatory Powers Act 2000 (RIPA)

In addition, the School is duty-bound to have regard to the following codes of practice:

The *CCTV Code of Practice* (Revised edition 2017 - version 1.2) published by the ICO

The *Surveillance Camera Code of Practice* issued by the Secretary of State under Section 29 of the Protection of Freedoms Act 2012

5. Responsibilities under the policy

All CCTV schemes that process personal data as defined by the GDPR and DPA require the identification of a Data Controller. It is the responsibility of the Data Controller to ensure the compliance of the scheme with all relevant legislation and the legal processing of the personal data generated as recorded images and audio by the systems. Where a CCTV scheme is run by a business or organisation such as the Council, it is the corporate entity that is the Data Controller rather than any individual member of staff. Therefore, within the context of this and other CCTV-related policies, the Data Controller is Pontarddulais Comprehensive School, as represented by the School's Management Team and its Data Protection Officer.

The GDPR requires a Data Controller who is processing personal information to register with the Information Commissioner as a Data Controller, unless they are exempt from the

requirement to do so. The School is registered on the Public Register of Data Controllers, a registration which is renewed annually. There is a requirement that any changes to the School's registration must be made within 28 days of the change. Failure to notify the Information Commissioner of this or the processing of personal information is a criminal offence.

It is nevertheless important at the outset to identify an officer who is or will be responsible for all practical aspects of managing the proposed CCTV scheme(s) on-site, including ensuring that in a day-to-day context the School complies and continues to comply with the legislation and codes of practice referred to above. This officer is to be designated as the Single Point of Contact (SPOC) for the system or systems.

While the day-to-day running of the scheme may be the responsibility of an individual member of staff or external agency representative ("operating officer") based on-site, the Data Controller still retains ultimate responsibility for the legality of the scheme and the SPOC for ensuring this compliance at a practical level (for example, the provision of adequate signage). The SPOC or operating officer could be committing a criminal offence if s/he were to act outside the explicit instructions of the Data Controller.

If the CCTV scheme is devolved to a third party such as a security company, the advice of the School as represented by the Data Protection Officer must be sought, and any explicit instructions about the operation, scope or limits of the scheme followed. This process is managed by means of a Data Protection Impact Assessment.

Where two organisations share a scheme, such as a live feed from one scheme to another, and both make decisions regarding its purpose and operation, then they both share responsibility.

The SPOC, or other person responsible for the day-to-day management of the scheme, has a number of responsibilities as outlined in this policy. Among these is the need to regularly carry out pro-active checks to ensure that this policy is being complied with, including a review of the on-going value and benefit of the scheme. If the scheme is not achieving its purpose it should be discontinued or modified.

A public space surveillance (CCTV) licence is required if CCTV is run by operators supplied under a contract for services. It is a criminal offence for staff to be contracted as public space surveillance (CCTV) operators without a Security Industry Authority (SIA) licence.

6. Means of Contact

There must be a single means of contact for members of the public, which is to be identified on signage in any area or areas covered by the CCTV camera(s). The means of contact (which is currently identified as a web address and online enquiry form, combined with a telephone number for those without online access) must be available to the public at least during office hours. All employees receiving comments, complaints, Subject Access Requests and other

communications through this single means of contact must be conversant with this policy and procedures governing data protection and the use of CCTV equipment.

Enquirers using this single means of contact must be provided if it is requested with one or more of the following:

- a copy of this policy
- a Subject Access Request form
- a CCTV complaint form
- information about the Corporate Complaints procedure

The Corporate Complaints procedure is only to be used if the member of the public wishes to pursue their concern about the use of the system, or about non-compliance with the Code of Practice and/or this policy, beyond a Stage 1 complaint.

A record of the number and nature of complaints and enquiries must be maintained, together with an outline of the action taken in response. A report of these figures must be produced regularly in order to assess public reaction to and opinion of the scheme(s).

7. Need for a CCTV Scheme

While there is a high level of public support for CCTV schemes, there are increasing concerns about the role of CCTV in a 'surveillance society'. In order to maintain public support and trust, it is important to ensure that the CCTV scheme:

- is established on a proper legal basis and operated in accordance with the law
- is necessary to address a pressing need, such as public safety, crime prevention or national security
- is justified in the circumstances
- is proportionate to the problem that it is designed to address

For existing systems, a Data Protection Impact Assessment (DPIA) *may* be required to determine whether the use of CCTV continues to be justified. For completely new CCTV systems (i.e. not a replacement or an upgrade of existing cameras), a DPIA is mandatory. Any impact assessment should consider the following:

- What is the purpose for using CCTV?
- What are the problems it is meant to address?
- What are the benefits to be gained from its use?
- Can CCTV technology realistically deliver these benefits?
- Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Are images of identifiable individuals required, or could the scheme use other images not capable of identifying individuals?
- Could more privacy-friendly options be used instead, such as only recording events likely to cause concern, such as movement in a defined area?

- Will the scheme being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Have the views of those who will potentially be under surveillance been canvassed and their views taken into account?
- What could be done to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

The Surveillance Camera Commissioner has published a template for carrying out a DPIA which also provides guidance on what DPIAs are and how they can be used to identify and reduce privacy risks associated with CCTV surveillance. The code of practice is accessible at https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras The School has adopted this template as its standard format for producing any CCTV-related DPIA.

8. Purpose of a CCTV Scheme

There are four categories for identifying the purpose for CCTV cameras:

● **Monitoring:** to watch the flow of traffic or the movement of people where it is not necessary to pick out individual figures
● **Detecting:** to detect the presence of a person in the image, without needing to see their face
● **Recognising:** to recognise somebody who is known, or to determine that somebody is NOT known
● **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Under this policy, CCTV schemes can be employed for the following purposes:

- Prevention, investigation and/or detection of crime
- Apprehension and/or prosecution of offenders
- Public and employee safety
- Traffic flow monitoring

The purpose of the CCTV scheme must be documented, and also the reasons identified why CCTV is the most appropriate means of meeting the scheme's objectives. It is not acceptable to extend the purpose of the CCTV scheme without altering its documentation, except where such evidence is required for criminal or other legal proceedings. For new schemes, the standard way to document the purpose of a CCTV scheme is through the DPIA process and, where a proposal is made to alter the purpose of the scheme to encompass broader aims, this is also suitable for a DPIA.

Once the purpose of the scheme has been identified, it is necessary to:

- ensure that everyone associated with the scheme is fully aware of its declared purpose, and the privacy implications of its use.
- ensure that the equipment is only used to achieve the declared purpose.
- decide whether constant real-time recording is required or whether motion activation or recording during specific time periods (such as out of hours) may be more appropriate.

The image quality required for each of these purposes varies – further information on this and assistance in selecting equipment is available from the Home Office Scientific Development Branch.

If the equipment used also records sound, this must not be used to record conversations between third parties, although there are some limited circumstances in which audio recording may be justified, subject to sufficient safeguards. Any use of such technology must be subject to a DPIA.

9. Location of Cameras and Microphones

The location of the CCTV equipment is very important and must be planned carefully. The physical spaces to be covered must be clearly identified, and the way in which records are gathered must comply with data protection principles as follows:

- Cameras and microphones must only monitor those spaces intended to be covered.
- Cameras and microphones must be situated to ensure that they will effectively capture recordings relevant to the scheme's purpose.
- If there is a risk of neighbouring spaces being monitored unintentionally, the owner of such spaces must be consulted.
- Adjustable cameras must be restricted to prevent operators from being able to allow unintended spaces to be viewed and/or recorded.
- Cameras must be able to produce images of sufficient size, resolution and frames-per-second
- Microphones must be able to produce audio recordings of sufficient quality and clarity.
- Physical conditions and environment must be borne in mind when siting cameras and microphones, for instance taking into account lighting and the size of the area to be monitored.
- All necessary steps must be taken to protect the cameras and microphones from vandalism and theft.

It should also be noted that some areas have heightened expectations of privacy, such as changing rooms and toilets, and cameras and microphones must only be (if ever) used in most exceptional circumstances to address very serious concerns.

10. Signage

In order to comply with the legislation and codes of practice referred to above, areas covered by CCTV schemes must display signs warning members of the public that CCTV is in operation. To comply with the School's adherence to the Welsh Language Standards, these signs should be bilingual. A suitable standard sign is available from the Council's in-house print unit.

The wording and location of signage must take into account the following points:

- Signs must clearly identify to the public when they are entering an area covered by CCTV. These signs can be supplemented with further signs inside the area of required.
- Signs must be clear and legible both in terms of lettering and size, appropriate to the sign's location.
- Signs must clearly identify:
    - Who is responsible for the scheme (i.e. the Data Controller)
    - The scheme's purpose
    - Details of who to contact about the scheme.

In exceptional circumstances, it may be agreed that signage may compromise the purpose of the scheme. In such cases the owner of the scheme must consult with the Data Protection Officer and Legal Services and must identify and document the reasons behind this decision, for example.

- A specific criminal activity for which there is a need to obtain evidence, for example illegal fly-tipping
- The reasons why signage would prejudice success in obtaining such evidence.
- How long the monitoring should take place to ensure that it is not carried out for longer than necessary.

In an area where public announcements are already being used, the message contained on the signs can be backed up with periodic audio announcements.

11. Equipment Quality

Procedures and systems must be established to ensure that CCTV equipment is adequately maintained, and that the quality of images recorded consistently meets the purpose of the scheme.

- Any tapes or other media used must be of good quality.
- All CCTV systems must comply with the relevant British or International Standard in force at the time. These are currently BS EN 62676-4:2015 and NSI NCP 104 Issue 3. This policy can be updated to reflect changes to these Standards without requiring resubmission of the policy for approval.
- Recorded pictures and prints as well as live screens must produce good quality images, and the quality must be regularly monitored.
- If the system records information such as date, time and camera location, this data must be accurate at all times.

- Equipment must be capable of being set up in such a way as to avoid inadvertent corruption.
- If an automatic facial recognition system is used to match images, those images must be of a sufficiently high quality to ensure accurate matching. All matches must in any case be verified and documented by a human operator.
- Selection of equipment must ensure that copies of a recording can be made easily if asked for by a law enforcement agency, and their use of the images should be straightforward.
- A maintenance log must be maintained for all equipment associated with the scheme.
- If a camera is damaged, there must be clear procedures for:

    - Defining who is responsible for ensuring repair/replacement.
    - Ensuring the camera is repaired/replaced within a specific time period.
    - Ensuring the monitoring and documentation of maintenance work.

12. Data Storage and Access

Retention periods must be established for required and non-required recordings, and secure and controlled storage and access arrangements for recordings in compliance with the principles of data protection. Any requirement for regular extensive retention (i.e. over the standard period of one month) must be discussed with the Data Protection Officer and subjected to a DPIA.

Any DPIA relating to extended storage of CCTV footage must take into account the following principles:

- Required recordings must only be retained for a length of time appropriate to their purpose and the purpose of the scheme. Non-required recordings must be erased as soon as practicable, being permanently deleted through secure methods.
- Systematic checks must be carried out to ensure compliance with the agreed retention period.
- When the documented period of retention has been reached, recordings must be removed / erased.
- Any recordings that are to be retained as evidence must be kept in a secure location with controlled access.

- When recordings are removed for use in legal proceedings the following information must be logged:
    - Date on which recordings were removed.
    - The reason why they were removed.
    - Any relevant crime incident number.
    - The location of the recordings.
    - Signature of the collecting police officer (if relevant).
- Monitors displaying images from areas where people would expect privacy must only be capable of being viewed by authorised employees of the User.

- Access to recordings must be restricted to the designated member of staff responsible for the scheme who will decide whether to allow disclosure to third parties in accordance with the scheme's disclosures policy.
- Any viewing of recordings must take place in a restricted area with controlled access.

When recordings are removed for viewing purposes the following information must be logged:

- Date and time of removal.
- Name of person removing the recordings.
- Name(s) of the person(s) viewing the recordings. If this includes third parties, it must also include the third party's organisation.
- The reason for the viewing.
- The outcome, if any, of the viewing.
- The date and time recordings were returned to the system or to a secure area.
- All operators and others with access to recordings must be aware of the access procedures that are in place.

13. Disclosure of Recordings

The SPOC and/or operational officer must ensure that access to, and disclosure of, recordings made by the CCTV system is restricted and carefully controlled.

The SPOC or operational officer must ensure that all employees are aware of the following disclosure and access restrictions:

- Access to recorded recordings must be restricted to those who need to have access to achieve the purpose of the CCTV scheme.
- All access to recordings must be logged and documented.
- Disclosure of recordings to third parties must only be made in limited and prescribed circumstances.
- All requests for access or disclosure must be recorded. If access or disclosure is denied the reason must be documented.
- If access or disclosure of recordings is allowed then the following information must be logged:
    - The date and time at which access was allowed or the date on which disclosure was made.
    - The reason for allowing access or disclosure.
    - The extent of the information to which access was allowed or which was disclosed.

Recordings must not be made more widely available other than through a police or Subject Access Request. If it is intended that they will be made more widely available (for example, for training purposes or a media request) that decision must be made by the SPOC or operational officer and the reason for the decision must be documented.

Where recordings have been copied to a third party, the third party becomes the Data Controller for their copies of the recording/s and are responsible for compliance with the GDPR and the DPA.

If recordings are to be disclosed to the media, the images of individuals must be disguised or blurred to ensure that they cannot be readily identified. If the system does not have the facilities for this kind of editing, a third party or company can be used. In such cases, the responsible member of staff must ensure that.

- There is a contractual relationship between the Data Controller and the third party or company.
- The third party or company has given appropriate guarantees regarding security measures they take.
- The Data Controller has checked to ensure that those guarantees are met.
- The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the Data Controller or designated member of staff.
- The written contract makes the third part or company's security guarantees explicit.

If staff are unable to blur or disguise the images of third parties in the recordings, the permission of all third parties captured in the recordings should be sought wherever possible.

15. Access to Recordings by Data Subjects

All staff involved in operating the equipment must be able to recognise and validate a request from a member of the public for access to recordings of the data subject. This validation process involves having photographic ID of a sufficient standard to be able to identify the data subject from the footage. Where such information is lacking, a subject access request cannot be progressed.

Data subjects must be provided with a specific CCTV Subject Access Request form which will:

- Indicate the information required in order to locate the relevant recordings.
- Indicate the information required in order to identify the person making the request. If the data subject is unknown to the equipment user, as well as appropriate ID verification a photograph of the individual will be requested in order to locate the correct image.
- Indicate that the response will be provided promptly and in any event within one month of receiving the request.
- Explain the rights provided by the GDPR and the DPA.

All Subject Access Requests must be dealt with by the SPOC or operational officer, who must also locate the recordings requested. S/he must also determine whether disclosure to the individual would entail disclosing recordings of third parties, and whether those third party recordings are held under a "duty of confidence".

If third party recordings are not to be disclosed, the responsible Manager of the CCTV system must arrange for the third party recordings to be disguised or blurred. If the system does not have the facilities for this kind of editing a third party or company can be used.

In such cases, the designated Manager of the CCTV system must ensure that:

- There is a contractual relationship between the Data Controller and the third party or company.
- The third party or company has given appropriate guarantees regarding security measures they take.
- The Data Controller has checked to ensure that those guarantees are met.
- The written contract makes it explicit that the third party or company can only use the recordings in accordance with the instructions of the responsible member of staff.
- The written contract makes the third party or company's security guarantees explicit.

If the member of staff responsible decides that a Subject Access Request is to be refused, the following information must be logged:

- The identity of the individual making the request.
- The date of the request.
- The reason for refusing to supply the requested recordings.
- The name and signature of the manager or designated Manager of the CCTV system making the decision.

If there is any doubt about whether recordings should be disclosed or access refused, the Data Protection Officer and the Council's Legal Services must be consulted.

It should also be noted that in addition to requesting the disclosure of recordings, individuals also have the right to request the School (by notifying the School in writing) to cease or to not begin processing images or recordings containing personal data likely to cause "substantial and unwarranted damage or distress". Advice on this aspect can be sought from the Data Protection Officer and Legal Services.

16. Compliance

The Information Governance team will periodically assess corporate compliance against this policy, reinforced where appropriate by external audit from IPCO.

Compliance with this policy is a term and condition of employment. Failure to comply with corporate policies is a potential disciplinary matter which may result in withdrawal of an officer's access to corporate systems. It may also lead to disciplinary action, up to and including dismissal where a gross misconduct has taken place.

17. Monitoring and Review

Monitoring for changes of this policy is the responsibility of the Data Protection Officer, who will ensure on-going monitoring and audit of the processes / guidance in place under the policy.

Changes to the attached schedule or any staff guidance documents are the responsibility of the Data Protection Officer and will be dependent on, for example, changes in technology, local procedure, legislation and the School's computer/network infrastructure.

18. Schedule of CCTV systems in operation

A schedule or inventory of CCTV systems operated by the School is attached at Appendix 1 and Appendix 2. This inventory may be updated and otherwise varied from time to time in order to keep it current without requiring reference back to the policy or the re-submission of the policy for approval.

19. Operation of CCTV systems within communal toilet areas

That the school will operate CCTV within pupil communal toilet areas throughout the School and subject to the control measures outlined in Appendix 3.

Appendix 1

REGISTER CCTV SYSTEMS (as at March 2024)

Service Unit	Section	Location	Total no. cameras
Education	Pontarddulais Comprehensive School	Front LH Entrance Front RH Entrance Humanities H1/H2 entrance Humanities H3/H4 entrance Humanities Stairs LH Humanities Stairs RH Humanities 1st Floor LH Humanities 1st Floor RH Humanities Ground Floor LH Humanities Ground Floor RH Humanities yard Red Gra Quad Leisure centre entrance English corridor Room 8 corridor Room 10 corridor Library corridor Pedestrian gate Drama corridor Food queue DT corridor Drama English Office junction Biology corridor Reception Leisure centre junction Business corridor Art corridor IT support corridor	1 in each area unless otherwise stated and 62 in total

		Staff room corridor Biology 1st floor corridor French corridor Library Welsh corridor Room 16 corridor Room 17 Room 19 Room 23 Room 26 Room 31 Room 46 Room 48 Room 48 rear Room 48 gates Room 48 front Main hall Main hall 2 Sports hall Gym Gym counter Gym lobby Field Outdoor changing room entrance PE / Leisure corridor Sports court 2G entrance 2G RH 2G LH Main car park Main car park 2 Pedestrian drive	
		IT network room own system	2

Appendix 2

CCTV in Toilet Areas

Service Unit	Section	Location	Total no. cameras
Education	Pontarddulais Comprehensive School	Year 8 Boys' Toilets	2
		Year 8 Girls' Toilets	1
		Year 9 Boys' Toilets	1
		Year 9 Girls' Toilets	2
		Year 10/11 Boys' Toilets	2
		Year 10/11 Girls' Toilets	1

Appendix 3

Control Measures in respect of use of CCTV in Pupils Communal Toilet Areas

1. That consultation will have taken place with pupils, staff, parents, appropriate Local Authority departments and the Governing Body.

2. That the operation of CCTV will have been approved by the Governing Body prior to implementation.

3. That year group toilets be designated for boys and girls throughout the school and currently being Year 7, Year 8, Year 9 and Years 10/11, which could be subject to review depending on the cohort size and any other operational factors which could require a change to the designation.

4. That the CCTV Policy will be reviewed on an annual basis by the Governing Body and be made available on the school website.

5. That the school will have prepared a Data Protection Impact Assessment (DPIA) which will help identify and minimise the data protection risks of the project. The DPIA will have been reviewed by the Local Authority Data Protection Officer prior to being considered by the Governing Body. Once approved by the Governing Body the DPIA will be held on file and made available should it be requeste by a third party.

6. That in respect of the DPIA, where the school was unable to mitigate against specific risks, then the school would contact the Information Commissioner's Office if advised to do so by the Local Authority Data Protection Officer.

7. That access to the CCTV system be limited to designated members of staff subject to an enhanced DBS being in place. This would include the School's Child Protection Officer, the Deputy School's Child Protection Officer, members of the extended Headship Team but excluding the Resources Manager.

8. That in the event of a designated member of staff leaving the organisation, then that person's access/password would be deleted from the system by the service provider who would have administration rights (PES Security Systems).

9. That female members of staff would view footage of the girls' toilets. A male member of staff would only view the footage if deemed appropriate to do so by the female members of staff.

10. That male members of staff would view footage of the boys' toilets. A female member of staff would only view the footage if deemed appropriate to do so by the male members of staff.

11. After viewing CCTV footage, additional support may be required from key members of staff, if appropriate, e.g. to identify pupils. The viewing of such footage from the key member of staff would only happen in the presence of designated members of staff.

12. That the number of cameras in each area will be determined by the amount of coverage required. Where there is only one camera in an area, this will be reviewed should there be vandalism to that camera and it deemed beneficial to have a second camera to identify such vandalism. The purpose of the additional camera would be to allow one camera to monitor the other.

13. That access to the system will be password protected and will be subject to a two-factor authentication. That means that no one member of staff will be able to access the system on their own.

14. That data will only held on the CCTV unit itself. No data will be transferred elsewhere unless explicitly requested by an authorised user (for example the police). The system will be on a stand-alone network.

15. That this will be a stand-alone system and not linked to the school system or the internet.

16. That the CCTV unit and screen will be in the Resources Manager's office who will not have access to the system. When the office is unoccupied, then the room will be always locked. When footage is being viewed, then the only persons viewing will be those that are authorised to do so. CCTV coverage is in place which will show those members of staff entering/leaving the office.

17. That the use of mobile phones will not be allowed when viewing CCTV footage.

18. That the data will be retained for a period of 30 days unless requested as part of an incident and certainly no longer than deemed absolutely necessary (for example the police).

19. That the 'blocking/screening off of the cubicles and urinals' (privacy masking) would be done using specialist software and would be subject to approval by the Local Authority Lead and Deputy Child Protection and Safeguarding Officers.

20. That the privacy masking, once set, will not fail even in situations such as power being restored following a power cut. The masking can only be set up, changed, and removed through the menu on the CCTV Recorder which is password protected and can only be accessed by authorised operators of the system (PES) who retain the administration rights. These changes to the privacy settings cannot be done remotely by PES who would need to attend site, with prior consent, and therefore be provided access to the office by the school. **That changes to the masking cannot be done by members of school staff.**

21. That in order to prevent malware/hacking of the data, the system will be air gapped and stored in a secure location, Resources Manager's office.

22. That there will specific signage in each toilet area, which advises that CCTV monitoring is operational within the area. The signage will be clearly visible on entry and within the toilet area. That the signage be robust and put up in a way that would be difficult for pupils to remove.

23. That the CCTV will be motion activated and will only commence recording once someone enters the toilet area. The cameras will be recording but not live streaming and can only be viewed on playback via password access with a two-factor authentication in place. There will not be any live images displayed on any monitor at any time. There will be no audio recording.

24. That a log will be maintained of each time the system is accessed and by which members of staff.

25. That the system will be reviewed after a period of 6 months to monitor its impact on the safeguarding of pupils based on the intended purpose of the installation.