Design and Technical Requirements - Security Systems

Content for inclusion in EFSG DTRs

Disclaimer

This document outlines Design Requirements and Technical Requirements, as they relate to Security Systems, for inclusion within the EFSG.

These requirements are to be used in conjunction with the relevant Vision and Objectives.

The information within this document once printed/exported will be classed as an uncontrolled copy. Its currency must be checked by visiting the EFSG/Technical Standards website prior to using the information for any purposes.

Document control

Document version: 0.2

Published date: 30th August 2024

Issued to: David Bennett, Technical Standards Team

Version history

Version	Date	Description	Prepared by	Approved by
0.2	30 August 2024	Final Draft DTRs	Jasna Stajic	
0.1	16 August 2024	70% Draft DTRs	Jasna Stajic	

Design and Technical Requirements - Security Systems

Purpose

The intention of this document is to outline essential conditions or functional attributes that transform ideas (vision & objectives) into clear and actionable design features.

High level design requirements (DR) allow for projects to understand the performance level they are to achieve – leaving space for innovation with technical requirements. Technical requirements (TR) provide a prescriptive way to meet safety and security requirements, objectives and vision.

Design requirements (DR) are essential conditions or functional attributes that transform ideas (vision/objectives) into clear and actionable design features. These requirements must be unambiguous and can include conditional elements.

Technical Requirements (TR) are prescriptive solutions that deliver design requirements, objectives, and vision to meet user functional needs.

Key Terminology

Acronyms and abbreviations can be found in the central EFSG Glossary, the following terminology is relevant to the Design and Technical Requirements (DTRs) within this document.

Crime Prevention Through Environmental Design (CPTED) is a multidisciplinary approach to crime prevention that focuses on using environmental design strategies to discourage criminal behaviour and enhance security of the built environment.

The "Defense in Depth" strategy is a comprehensive approach to security design that uses multiple security layers to protect assets and to efficiently manage risks.

Security systems within this document relate specifically to technology-based security solutions integrating electronic components such as intruder detection/alarm system, CCTV and electronic access control.

Primary Security Line in schools includes perimeter security measures that form the first line of defence against potential threats, ensuring efficient security and preventing unauthorized access.

Secondary Security Line represents additional layer of defence beyond primary security measures introduced to control access to designated parts of the school site.

Target Hardening refers to security measures applied to external envelope of the building, to external walls, windows and doors.

1. Security Risk DTRs

(DR) A security risk assessment must be undertaken for each school site at the early stage of the project.

(DR) Schools shall be designed to ensure a safe and secure built environment while maintaining a welcoming and conductive learning experience.

(DR) Security Risk mitigation must safeguard both occupants and school property from external threats and risks.

(DR) Security risk mitigation strategy must implement a range of measures, integrating technologies and developing physical infrastructure to create secure educational environments.

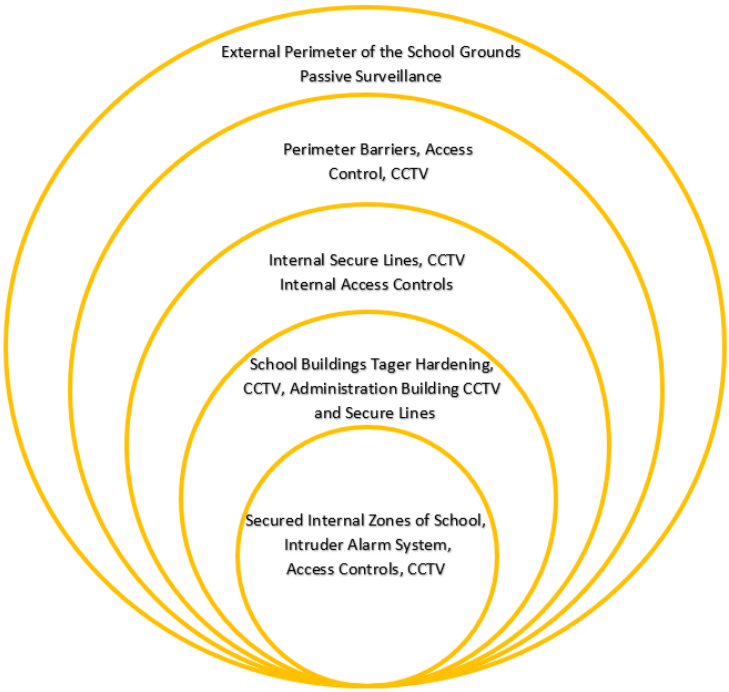
(DR) Security risk design must include extensive consultation to determine the most effective solution for each site, relevant to its context.

(DR) Security design must include a comprehensive risk assessment in conjunction with CPTED (Crime Prevention Through Environmental Design) principles

(DR) Security design for school sites must incorporate a "Defense in Depth" strategy by implementing multiple layers of security measures.

(DR) Design approach must integrate passive surveillance from the external site perimeter with both physical and electronic barriers to enhance the resilience and effectiveness of the school security.

Figure 1. “Defense in Depth” Diagram for typical School Site



2. Physical Barriers and Perimeter Site Security DTRs

(DR) The primary security line in schools must include perimeter security measures that form the first line of defence against potential threats, ensuring efficient security and preventing unauthorized access.

(DR) Primary security lines of the school must integrate physical security barriers and electronic security systems. Physical barriers shall include secure fence, gates, building structure and landscape treatment, while electronic systems shall integrate CCTV, intruder alarm systems and electronic access control at entry points.

(DR) Buildings shall be set back from the site boundary to allow for secure fence installation whether as part of the initial construction or future implementation.

> **(TR)** Secure fencing shall be minimum 2.1 m high and 1.2m minimum distance away from potential climbing points such as handrails, service meters and other utilities, steps, ramps, brick walls etc.

(DR) Each school site shall have appropriate number of pedestrian and vehicular entry points, secured with gates and electronic access control and integrated with the School Intruder Alarm System reporting back to Central Services Control Monitoring Centre (CMS).

(DR) School gates shall be designed for mass movement of students and shall be open during school start and finish time.

(DR) During school hours, gates shall be closed, and perimeter fence shall be secured to prevent unauthorized entry or exit utilizing electronic access controls, managed by school staff inside the Administration Block clerical office.

(DR) All access controlled gates shall be monitored by CCTV cameras for staff in the Admin clerical office to manage visitor's access at the perimeter boundary.

(DR) Wayfinding signage shall be incorporated to direct visitors to the main pedestrian entrance gate and the public reception at Administration office.

(DR) Where building forms a primary security line of the school, additional security measures are required, including the following

> **(TR)** Target hardening measures to the windows below 2100mm height on external façade at the perimeter of the school site - grilles, security mesh or security film.
>
> **(TR)** All general doors shall be solid core with steel frames
>
> **(TR)** Target hardening measures to the glazed doors to Administration entry - application of grilles, security mesh or film.
>
> **(TR)** Anti-Graffiti treatment shall be used to protect to external walls facing public domain
>
> **(TR)** Additional CCTV coverage on interface of the building and public domain
>
> **(TR)** Additional external lighting on interface of the building and public domain
>
> **(TR)** Suitable landscape treatment shall be considered to prevent unauthorized access to the building.

(DR) Secondary security line must include both physical barriers and electronic access control measures.

(DR) Administration block must be located adjacent to the main entrance of the school. It shall be easily accessible from the school parking and shall have direct access from the main pedestrian entry.

(DR) Access to the Administration Block must be designed to direct visitors to the public reception area without granting them access to other parts of the school.

> **(TR)** Provide physical barrier (fence or wall structure) along pedestrian walkway between main entrance and Administration block to protect unauthorized visitors' access to the school site.

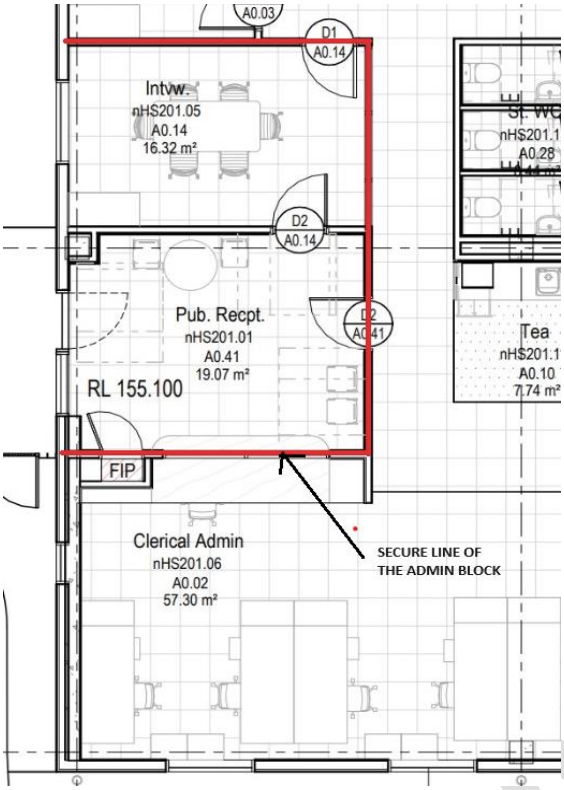
(DR) Administration block shall be designed to separate Public Reception**,** accessible to school visitors, from the secure areas used by school staff.

> **(TR)** Secondary security line in Administration Block must integrate physical barriers (partitions, doors, fixed glazing) with electronic access controls.
>
> **(TR)** Include physical barrier in the form of glazed partition at the visitors' reception counter to protect clerical staff from hostile intent.

(DR) The public reception area should have direct access to the adjoining dual-access interview rooms. The layout of these interview rooms must be designed to allow access from both the public reception and secure staff areas, with restricted access doors installed to ensure security.

(DR) The layout of an interview room and room furnishing must provide an obstruction between visitors, staff members and the interview room egress door.

Figure 2. Secondary Security Line of the Administration Block



(DR) Out of Hours School Care and Pre School facilities must be considered as a separate entity and must have secondary security lines of their own. This applies to new and existing schools, taking into consideration master planning and layout of the specific school sites.
(DR) Access to joint and shared use facilities shall be tailored to specific school's needs without compromising existing security measures.

(DR) Shared and joint use facilities shall be situated near the perimeter of the school site, with direct access from the entrance gate and secure separation from the rest of the school.

(TR) Provide appropriately sized gates to allow direct access between school and shared facilities.
(TR) Provide emergency exit directly from the school grounds for users of the shared and joint use facilities.
(TR) CCTV cameras are to be installed in the shared and joint use facilities to monitor and record access.
(TR) Electronic access gates shall be installed to the entry leading to the shared and joint use facilities.

3. Electronic Security Systems DTRs

(DR) Electronic security systems, including intruder alarms, CCTV surveillance and electronic access control shall be integrated into a cohesive network and will be centrally managed and monitored.

(DR) Electronic equipment is to be installed in locations and positions that allow the system to operate at maximum effectiveness and not to be obscured or impeded in operation.

(DR) Security system design must take into consideration surrounding fixtures and fittings such as blinds, curtains, fans, air conditioning ducts/vents, doors, joinery and furniture which might impact functionality of the electronic security equipment.

(DR) Electronic components of the security system must not be exposed to adverse environmental conditions or foreseeable risk of damage through vandalism or accident.

> **(TR)** Any ducts, conduits or cable paths forming part of the security system are not to have other services installed in them.
>
> **(TR)** All installations are to be “turnkey” and provide all necessary work to support the security system to function as intended.
>
> **(TR)** All equipment must be of a commercial quality, sourced from reputable Australian distributers, be readily available for any other industry contractors to service them and be non-proprietary.
>
> **(TR)** All equipment is to be of brand and model approved by the NSW DoE prior to tender response and construction.
>
> **(TR)** All devices and systems are to be hardwired unless specified or formally approved by the NSW DoE.

3.1 Intruder Detection (Alarm) Systems

(DR) Intruder Detection systems must provide instantaneous detection of unauthorised access attempts or intrusions into school buildings.

(DR) Alarm system components must be installed in a manner that would prevent possible tampering and minimize vandalism.

(DR) System shall be designed for easy expansion and future upgrades and will be integrated with any existing networks.

(DR) Intruder detection on each school site must be integrated into a unified system. Each site is permitted to have only one callout alarm panel, standalone systems are not allowed.

(TR) All alarm systems in DoE schools are monitored by the Central Monitoring Station (CMS). The alarm system shall be compatible with the NSW DoE's existing remote management software and be able to transmit alarms to the NSW DoE monitoring station using communication modules supplied by DoE.

(TR) Alarm Head End/Control Panel requires network connection and shall be capable of communication with the Central Monitoring Station (CMS).

(TR) Control panel shall be installed in the Main Communication Room (MCR).

(TR) Main Communication Room (MCR) is to be secure and protected by the intruder alarm system.

(TR) Auxiliary modules are to be placed in secured areas with lock and key, such as building distributers or storerooms, suitably protected by the intruder alarm system.

(TR) Auxiliary modules are to be wall mounted.

(TR) Module enclosures must be mounted at a height not less than 700mm above finished floor level (AFFL) to the bottom of the enclosure, and no more than 2000mm AFFL to the top of the enclosure.

(TR) Each module enclosure is to have an area of 150mm clear space at either side of the enclosure and 1000mm at the front to allow adequate space for service personnel.

(TR) When module enclosures are mounted side by side, it is allowed to install them hard against each other, without any clearance.

(TR) Control panel, expanders and access control modules must be of a type, model, and brand approved by DoE.

(TR) Control panel, expanders and access control modules must incorporate a smart power or endorsed power supply with a minimum of 3A capacity and back up battery inside the enclosure.

(TR) Input expander panels will be capable to expand to 32 input and will be fitted in suitable enclosure size to facilitate the expansion. Minimum medium size enclosure must be provided.

(TR) The RS-232 Local Area Network (LAN) for the intruder alarm system is to be a dedicated copper cable.

(TR) Active, passive, wireless or fibre devices are not to be used for system LAN.

(TR) System LAN cabling is to be installed in a star configuration between blocks for Alarm/Access control modules and Alarm head end location.

(TR) All security cabling on a site shall emanate from a central location at the control panel LAN Termination Box (LTB) in the MCR and run to each device.

(DR) Motion detectors shall be installed to detect movement in internal spaces of the building and must not be placed in external or open facilities where environmental factors can cause false alarms.

(DR) Internal movement detectors shall be installed in:

- Internal circulation corridors and stairs
- Internal rooms and areas

(DR) Internal movement detectors shall not be installed in

- Wet areas including cleaners' storerooms, toilets and bathrooms
- Any plant rooms
- Kiln rooms

(DR) Internal areas are to be completely covered by the movement detector range.

(TR) Install more than one movement detector to large or irregular shaped rooms to achieve complete detection coverage, depending on the size and orientation of the room.

(TR) Provide additional motion detectors for the rooms that have internal fit out or furniture which restricts detection coverage.

(TR) In rooms where detectors are obscured by shelving or inbuilt joinery, 360° style ceiling mounted detectors must be installed to achieve complete detection coverage

(TR) Motion detectors shall have a minimum range of 12m and shall have a minimum 90° detection pattern.

(TR) Each motion detector must be installed at minimum 2600mm height relative to the floor finish level, so it is not easily reached, vandalized or obscured.

(TR) Motion detectors installed in DoE facilities shall be:

- Wall mounted sensors or
- 360° ceiling mounted sensors

(TR) Wall mounted detectors must be positioned in a corner of the room. They are to be installed at 45° from the corner (“hard corner mounted”), positioned in a way that possible intruder entry paths are crossing the movement detection pattern.

(TR) When motion detector is installed in the area where there is a risk of physical impact and damage, it must be protected by a sturdy metal cage.

(TR) Motion sensors are to be directly fixed to the wall or ceiling.

(TR) An individual cable must run from each movement detector directly to the input expansion module.

(TR) Each movement detector must be connected to an individual zone input.

(TR) All motion sensors are to have inbuilt tamper functionality.

(TR) When installed in rooms where exposure to dust and moisture is expected, movement detectors shall have a minimum ingress protection rating of IP54.

(DR) Reed switches (electro-magnetic sensors) are to be fitted to all doors leading to external areas, including open verandas and courtyards, with exception to toilets and changerooms.**(TR)** Reed switches must be installed to

- External doors
- Roller doors (including canteen shutters)
- Electronic Access Gates (both pedestrian and vehicular)

(TR) Reed switches on standard doors must be 20mm concealed flush mount type.

(TR) When door frame or door is constructed from, or sheeted with metal, suitable metal door reeds must be used.

(TR) An individual cable must run from each reed switch directly to the input expansion module.

(TR) Each reed switch must be connected to an individual zone input with exception of a dual leaf door where the reed on each of the two leaves is to be connected to a single zone input.

(DR) Internal screamers/sirens shall be installed in the internal areas of the building in the following locations:

- Minimum one internal screamer on each level of each block
- Administration area
- Library
- Hall
- Canteen

(DR) Large floors or blocks shall require multiple internal screamers as directed by DoE.

(TR) Internal Screamers shall be installed minimum 3m away from the keypad.

(TR) Screamers must be installed in a manner that shall prevent possible tempering and minimize vandalism.

(TR) When screamer/siren is installed in the area where there is a risk of physical impact and damage, it must be protected by a sturdy metal cage.

(DR) Local duress items (such as accessible toilet duress buttons) must be configured to operate locally, to the school only and shall not report to the NSW DoE Central Monitoring Station (CMS).

(DR) Keypads**,** used to arm and disarm the system (or specific parts of the system), shall be installed in the internal areas in the following locations

- Adjacent to the intruder alarm control panel for use by service personnel
- Secondary Local Area Network (LAN) Termination Board locations for use by service personnel
- Administration entry, staff common area entry, canteen entry
- Library entry, Hall entry, Gymnasium entry
- Each school block and ground floor main entry door
- Entry to OOSH and pre-school facilities
- Other areas designated by NSW DoE

(DR) Keypads are to be installed internally.

(TR) Keypads in publicly accessible areas and areas accessible to students are to be installed in approved lockable housing.

3.2 Electronic Surveillance Systems (CCTV)

(DR) Electronic Surveillance Systems shall be designed to monitor and record activities around entrances and high-risk areas of the school.

(DR) CCTV systems shall be designed to comply with

- Legal Issues Bulletin 41
- DoE Structured Cabling System Specification
- Functional Standards, Installation and General Requirements
- Other relevant standards and legislation.

(DR) CCTV systems for school facilities shall be installed in consultation with DoE security team, shall meet the design requirements of the school and be fit for purpose.

(DR) All equipment must be of a commercial quality, sourced from reputable Australian distributers, be readily available for any other industry contractors to service and be non-proprietary.

(DR) In case school has existing, previously installed CCTV camera systems, not compliant to the current version of DoE ICT Structured Cabling specifications, the project needs to identify this and allow the costing for supply, installation, replacement, rectification and reconfiguring works at design stage cost plan to avoid future variations.

(DR) CCTV cameras shall be installed in critical areas identified in consultation with the school or Security Projects Team including

- Pedestrian and vehicular entry/exit points
- All Electronic Access Controlled gates, by default
- External walkways
- Parking lots
- Bus pick up and drop off zone
- Playgrounds
- Lifts Lift wells (not internally on lifts)
- COLA and canteen
- Administration Block public reception area and sick bay

(DR) The only exception to the installation of CCTV at EAC gates is when there is a direct line of sight between EAC gate entrance and clerical office at Administration Block. Specific conditions and line of sight between the EAC gate and Clerical Office shall be investigated on case-by-case basis.

(DR) CCTV camera installed in Sick Bay, Administration Block, shall be on non-recording system, for live viewing purposes only.

(DR) CCTV cameras must not be installed in learning areas, student amenities, change rooms or other spaces where students and staff have a reasonable expectation of privacy.

(DR) DoE Security Notice and CCTV signage must be mounted to the security fence panel adjacent to each entry point leading into the school. In addition, a CCTV sign must be provided at each entry to buildings that have internal CCTV installation.

(TR) CCTV Cameras shall have unique Internet Protocol (IP) address and shall transmit video data over a network through DoE ICT field operations team for connecting devices over Security VLAN only .Central Services technicians shall be allowed to remotely connect to devices to provide maintenance support to schools

(TR) All CCTV systems shall be connected over the Security VLAN with the support of ICT Field Operations.

(TR) Recording Equipment via Network Video Recording (NVR) system on site must be provided.

(TR) Offsite, cloud, or decentralised systems are not permitted in DoE facilities.

(TR) The Network Video Recording system must have a minimum 32 channel capacity.

(TR) The NVR must be compatible with Open Network Video Interface Forum (ONVIF)

(TR) Recorded viewing must be available through the NVR or other approved software, installed in accordance with security guidelines.

(TR) Live Viewing shall be available through the monitors installed in Administration Block. Location of the monitors shall be determined in consultation with the school staff.

(TR) Recording set-up shall be configured for continuous recording at 20 fps minimum at full resolution.

(TR) Sufficient hard disk capacity to record all channels with a minimum retention period of 60 days + 20% must be provided.

(TR) CCTV cameras must be ONVIF compatible, non-proprietary and compatible with all electronic security systems.

(TR) CCTV cameras must have inbuilt illumination for 0 lux vision – minimum 30m.

(TR) CCTV cameras must have a minimum resolution of 6MP @ 20fps

(TR) CCTV cameras must have a vandal resistance rating as follows:

- Internal – IK08
- External – IK10

(TR) CCTV cameras must have an ingress protection rating as follows:

- Internal – IP55
- External and wet areas – IP66

(TR) CCTV cameras must have auto-iris and motorised vari-focal lenses suitable for the installation requirements.

3.2 Electronic Access Controls (EAC)

(DR) Access control systems shall be designed to integrate physical barriers, electronic access control, CCTV systems and visitor management protocols.

(DR) Electronic Access Control (EAC) systems shall be designed to manage entry to the school site, a building or specific area on the school site.

(DR) Access control devices shall be installed in locations that are of high risk and in the areas that require restricted access.

(DR) Security design shall identify areas on school site where EAC is required for a security purposes, including but not limited to

- Main pedestrian entrance
- Main vehicular entrance
- Secondary security line/s

(DR) Areas not suitable for EAC installation shall be identified during the design stage and alternative solution shall be proposed.

(DR) System shall be designed for easy expansion and future upgrades and shall be integrated with any existing networks.

(DR) EAC must be fully integrated with the Intruder Alarm System and CCTV.

(DR) Standalone CCTV systems are not permitted in DoE facilities.

(DR) Door control modules must be of the intelligent type, enabling the door controller to continue to operate in the last known programming configuration in case Local Area Network (LAN) system fails.

(DR) EAC readers and credentials are to be of the proximity type and non-proprietary.

(TR) EAC credentials (electronic fob “keys”) are to be site coded with the credential number referencing the programming clearly printed on the credential to minimise the chance of the number becoming un-readable over time.

(TR) Unless otherwise agreed and approved by DoE, allowance shall be made for the total number of credentials (fobs) in accordance with school requirement (number of permanent and casual staff, cleaners, contractors) plus an additional 50%. For example, if the school’s total staff number is 100, then 150 credentials shall be supplied. This quantity must be advised by the school prior to quoting or tender response.

(TR) Each user will have their access control credentials directly allocated to them and programmed into the system as individuals. Unused credentials are not to be active (will not operate any part of the EAC or intruder alarm).

(TR) EAC on doors must complement and must not change operational principals of door hardware as stipulated in Educational Facilities Standards and Guidelines (EFSG).

(TR) All EAC doors must have a manual key over-ride in case of electronic system failure.

(TR) EAC shall be limited to single leaf doors.

(DR) EAC and automation must be installed to purpose-built gates that are in good working order.

(DR) EAC is only to be fitted to single leaf/panel gates or sliding gates.

(TR) Motorised swinging gates must not be installed.

(TR) Where automated gates are designed for pedestrian use, trip hazards are to be avoided by using track-less styles (e.g. cantilevered gate panel).

(TR) Climb points due to the mounting of fixtures such as handles, card readers, safety sensors and intercom are to be eliminated.

(TR) When mounting of security equipment or door/gate hardware (e.g. push pull handles or protruding intercoms) introduces climb points, sufficiently angled shrouding must be installed to eliminate climbing risk

(TR) EAC system components at school entry (pedestrian or vehicular gate)

- Card Reader – both internal and external
- Video intercom – both external and internal
- Manual override with double sided key barrel, keyed to Education Security Master key series.
- Electric Strike lock – configured to fail secure.
- Reed Switch
- Self-closing mechanism or hinges
- Horizontal Broadhurst locking mechanism
- Wide angle viewing camera

(TR) External entry camera is to be displayed on a 42” monitor in the clerical area, enabling the staff to make an informed decision to unlock the gate ensuring there is no unauthorised person following an authorised person through the gate and that there are no inherent safety issues

(TR) EAC system at secondary security line in Administration Block shall include

- Card Reader - mounted in the public reception area, to restrict access to the interview room.
- Card Reader - mounted in the public reception area, to restrict access to the clerical office.
- Card Reader - mounted in the public reception area, to restrict access to the main school.

- Client awareness camera – mounted to view the reception area with the purpose to clearly identify visitors at the reception.
- Public awareness monitor – 32” monitor mounted in the reception area.

(TR) Request to Enter button should be mounted in the clerical office allowing staff to remotely allow visitor access from the reception foyer to the Interview rooms while maintaining visual line of sight from the clerical office.

(DR) Cabling pathways between buildings and other infrastructure (e.g. vertical cabling pathways/risers) are to be underground.

(DR) The security system cabling pathways should follow the structured cabling pathways.

(DR) Cable installed as part of the structured cabling system (such as CCTV, intercom, and Control Panel) is to comply with the DoE SCSS, formal testing certification is to be provided at the time of commissioning.

(TR) Where cables terminate to end of line devices (such as reed switches or proximity card readers) with tail-outs, the joints must be appropriately soldered and individually encased in suitable heat shrink. The entire termination shall be enclosed in heavy duty heat shrink to protect the joint as an outer sheath.

(TR) Cable joins/joints are not permitted;

(TR) All cables are to be a single factory manufactured length, end to end. In case cables be damaged the cable is to be reinstalled as one single continuous factory manufactured length.

(TR) All wiring and cabling is to be concealed.

(TR) Aerial/catenary cabling must not be used.

(DR) Conduit used for security cabling shall be dedicated to security only and not used for any other service.

(DR) Surface conduits along fences, paths, driveways, exterior of buildings or walkways are not to be used.

(DR) Pits used for security must be dedicated to security use only and must not be used for any other services.

(DR) Conduits and cabling are not to run through one building to reach another. Each building must be individually fed from underground pathways leading to the MCR.

(TR) Underground pathway conduits to are to consist of a minimum of 2 x 50mm conduits.

(TR) All cable entries into buildings are to have a P5 pit as close as possible to the building or a maximum of 5m from the building entry point.

(TR) External infrastructure such as gates or CCTV poles to have a P5 pit as close as possible or a maximum of 5m from the infrastructure.

(DR) All underground cable runs are to have pits at intervals of no more than 30m.

(DR) P5 pit must be installed at any significant change in direction of underground pathways.

(DR) If an underground pathway is to rise at retaining wall or similar, a P5 pit shall be placed at the top and bottom of the rise.

(DR) Bollards and poles, both internal and external, are to have a P3 pit located within 5m.

(DR) The P3 pit should feed back to the adjacent main underground pathway P5 pit within 10m.

(TR) At each pit location, a minimum of 1000mm of cable is to be neatly coiled and hung so as not to be sitting on the pit base.

(TR) The labelling system must be adhered to the component, be considered as permanent and last for the entire life of the device.