CCTV Policy Framework

The use of Audio-visual lesson capture, broadcast and surveillance technologies at TKIS

Since 2019, the school has been operating a high-quality digital recording and surveillance network on campus and in most classrooms. The following is information relevant to this decision for parents/carers.

In 2017, the board of The Kooralbyn International School, as part of a larger study into a Digital Literacy Grant application, commissioned the undertaking of an investigation into classroom lesson recording and their associated technologies. The investigation, overseen by the Principal, looked at recording/surveillance technologies from several perspectives including...

- their potential benefits – financial, pedagogical, administrative, security and safety, etc. (clearly the school was considering the technology for reasons well beyond just the traditional use of surveillance and security)
- the risks, privacy and legal implications of their deployment.

New 10Gbps optical fibre local area networks; new advancements in data capture, podcasting and storage technologies; smart imbedded video production and database-driven learning tools that can allow teachers to empower their students to take control of their own self-directed learning and assessment; etc., mean that a school today can bring together the power of self-directed learning, flipped classrooms, student-based work units and differentiated learning to accommodate a vast range of learning needs on one hand, while exploiting that same technology to improve accountability, child-safety, staff-safety, facility security and general communications on the other.

The school's review concluded that the benefits of the new technologies far outweighed their costs, that while they are already (early 2018) reasonably affordable, their cost-to-benefit ratios continue to improve every year and that the vast majority of negative perceptions about the use of such technologies seem to be based less on legal and financial fact and more on hearsay and rumour. For example, as long as everyone's rights to privacy in 'private areas' and in 'private situations' is maintained and that people are informed and reminded that all public areas of the school are likely to be monitored and recorded, the biggest problems associated with the use of these types of technologies is working out what happens to the data AFTER it is recorded.

There are slightly different legal ramifications pertaining to video (photographic) and audio recordings; to written information recorded within the process of lesson-capture; to music or other APRA or AMCOS copyrightable materials captured within the captured lesson's presentation; to recordings of students and staff versus recordings of parents or members of the public visiting the school; to data edited and produced for ongoing distance education programs versus data that is simply archived for WH&S or potential security purposes. Suffice it to say, the judicial use of this type of technology in a school, if carefully controlled and managed within a *clear policy framework*, can deliver genuine, long term learning benefits for our students.

*The **benefits** of using digital recording and surveillance technology in our school.*

1. **Service and product extension options**, particularly in relation to flexible learning alternatives, distance education, flipped classroom and differentiated learning for students with specific needs or students who miss large amounts of classroom contact.
2. **Greater subject options**, for students who would prefer to undertake subjects that are offered by the school but timetabled at the same time.
3. **Professional development and pedagogical improvement for teachers**, particularly in relation to peer review, mentoring and modelling practices, self-assessment, provisional to full registration processes and broader teacher-training and lesson efficacy considerations.
4. **Assessment and moderation evidence and justification options** in the form of access to a recorded portfolio of students' classwork that could be utilised to help justify gradings, drive internal moderation meetings or contribute to state panel submissions (or their ATAR equivalents).
5. **General classroom and behaviour management benefits**, particularly in relation to reducing (or at least deterring) inappropriate, unproductive or dangerous behaviour in the classroom and having referrable evidence to better manage disputes arising from accusations, counter-accusations and miscommunications that can occur in a complex social environment, like a classroom or school yard.
6. **Broader Workplace, Health & Safety gains**, particularly in relation to providing government required evidence that all relevant WH&S processes and policies are being followed by staff and students and to foster a culture that continually seeks to improve safety and eliminate discrimination in its workplace. (A case in point is the recent requirement from the school's certifiers to demonstrate how the school is managing vehicular speed on campus, etc.)
7. **Improved security for the school's assets and resources** by deterring vandalism and theft or at least providing actionable evidence which could improve the chances of recovery of lost or damaged property.
8. **Child Safety improvements** by maximising the scope, scale, equity and transparency of surveillance that the school is able to deliver and thereby (in line with the 'Child Safe Standards' proposed by the *Royal Commission into Institutional Responses to Child Sexual Abuse*) physically minimise the opportunity for abuse to ever occur. The new tamper-proof,

auto-archiving technologies support the school's need to maintain accurate records relating to child safety and wellbeing.

9. **Minimising public liability risks**, specifically in relation to things like WH&S, Child Safety, Duty-of-care obligations, public safety, etc., where there is now almost an expectation from the insurance and legal communities that schools and similar service providers WOULD be providing a carefully-managed security and surveillance system to help mitigate public liability risks.

CCTV Technology in Australian Schools

As long as schools use and control the data they record in strict accordance with the Australian Privacy Principles, (which are more concerned about making sure that data is not published or exploited in a way that undermines any person's legal rights to and expectations of privacy and it is not used by law enforcement entities unless duly sworn warrants are issued) then schools are protected by Australian and state law to make recordings including photographic, audio and text for educational, WH&S, child safety and general security purposes.

*The **risks** associated with using digital recording and surveillance technology in our school.*

There are several pieces of legislation and related recommendations (both state and federal) that can potentially impact on the use of recording and surveillance technologies in a school, including:

- *Child-Safe Standards* as advised by the *Royal Commission into Institutional Responses to Child Sexual Abuse*
- *Child Protection Reform Amendment Act 2017*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*
- *Work Health and Safety Act 2011*
- *Education and Care Services Act 2013*
- *Child Protection (International Measures) Act 2003*
- *Child Protection Act 1999*
- *Information Privacy Act 2009*
- *Privacy Act 1988*
- *Surveillance Devices Act 2004*
- *Copyright Act 1968*
- *Copyright Amendment Act 2006*

Child protection legislation among other things, requires schools to maximise their vigilance, supervision levels and transparency of reporting on all aspects of child welfare. Perhaps surprisingly however, very little of Australia's and Queensland's privacy and surveillance legislation has anything to do with schools using CCTV recordings of semi-public areas (like school grounds and classrooms). As long as schools use and control the data they record in strict accordance with the APP (Australian Privacy Principles, which are more concerned about making sure that data is not published or exploited in a way that undermines any person's legal rights to and expectations of privacy and it is not used by law enforcement entities unless duly sworn warrants are issued) then schools are protected by Australian and state law to have the right to make such recordings including photographic, audio and text for educational, WH&S, child safety and general security purposes.

Millions of videos are recorded on smart phones and published to social media and video sites daily. The prevalent laws addressing the use of such technologies on school grounds or within classrooms are the rules and policies set by the schools themselves who will normally prohibit such use (i.e. schools often prohibit staff or students from recording data on their own private devices (phones,

tablets, etc.,) while on school grounds, because of the school's lack of control over the potential misuse of such recordings and the school's subsequent risk of prosecution because of that misuse). In other words, the school is far more concerned about people's legal rights to privacy being violated through video/audio recordings that it has no control over (e.g. footage and images shot by people on their personal phones and uploaded instantly to social media sites), than data that it responsibly controls in strict compliance with the Australian Privacy Principles.

Other legal issues that had to be considered include…

- potential infringement of copyright or intellectual property; *[the school needs to declare on its annual CAL (Copyright Agency Limited) reports the use of any published works used in lesson capture or production for educational purposes]*
- publishing or profiting from work that includes a person's likeness without obtaining that person's (or the relevant parent/carer of a child's) written permission (referred to as 'obtaining a talent release'); *[Parents are required to sign TKIS student application forms which includes a release that allows the school to use photographic or other likenesses of their children for marketing or educational purposes] – [staff whose likenesses are used in the production of distance education or remotely accessed lessons (including flipped classroom resources) are required to sign a 'talent release'] – [all persons entering the property will be advised by clear signs that their activities will be recorded and entering the premises implies giving tacit approval to be recorded, etc.]*
- publishing a likeness (photo or video recording) of a child who has a court order or parental request in place, that prohibits promotion of the child's identity or location online. *[This issue is more complicated than whether the school has CCTV cameras on campus. For a start, the school publishes newsletters, online blogs and other promotional materials all of which need to be screened as a matter of school policy, to ensure that NO child is identified by full name – regardless of any instructions being in place. Also, as a matter of policy (i.e. the school's CCTV Policy Framework) no CCTV surveillance recordings made on school property, are **ever** published to the Internet, nor are they made available to anyone outside a strict process and policy designed to ensure people's privacy rights are maintained. In the event of in-class footage being utilised for lesson capture purposes, the school has technology that can remove the identity of anyone in the footage (pixelating algorithms that track faces, etc.) though clearly, teachers need to be informed about students who have 'instructions' in place, to make alternative arrangements in lesson capture situations.]*
- the question of: who holds and retains ownership of the material recordings and any works produced therefrom? *[Other than existing copyrightable materials that may have been included in the recordings, the works produced by school staff, on school property, during school time using school equipment, with school students… will otherwise remain the intellectual and material property of the school and potentially any other commercial stakeholder…software companies, state or federally funded programs, etc.]*
- clarification that persons entering the school grounds (see above points) must be clearly informed that the school employs digital recording technologies and that entering the property implies giving the school tacit approval to record any activities involving students, staff or school property in accordance with the *Information Privacy Act 2009*, the *Surveillance Devices Act 2004*, the *Work Health & Safety Act 2011*, the *Education and Care Services Act 2013* and the school's CCTV Policy Framework, etc.
- expectations by members of the public that they might have a right to view or obtain a copy of footage recorded by the school of themselves and/or other persons, e.g. a parent demanding to see footage of a teacher working in a classroom that their child attends. *[In fact, **no one** other than authorised personnel of the school and members of law enforcement who have obtained a duly sworn warrant, have a legal right to view, edit or copy data recorded by the school, and THAT's only within a **'clear policy framework'** designed to ensure*

that recorded data is managed in accordance with Australian Privacy Principles and Information Privacy Principles (Information Privacy Act 2009.]

- the notion that since the school is recording data in its *public areas*, there might be an expectation that the school will maintain such recordings for up to three (3) months. *[This is at least partially true. For example, law enforcement officers can apply to a court for a warrant to obtain an authorised copy of CCTV footage, so it's requested (as a matter of good practice) that such recordings should be kept for a minimum of 30 (thirty) days. Modern CCTV systems ensure that footage cannot be accidentally (or purposely) erased by the operator's staff, but that once the hard drives (storage) is full, new data will be recorded over the oldest data. As such, the length of time that a system stores its footage is a function of the amount of data it records every day and how much total storage capacity it has available. Authorised footage can be **copied** for editing for program production purposes, but the original data should not be deleted until the hard drives cycle is complete and hopefully if calculations have been performed correctly, that will not be for at least thirty (30) days from the time the data was originally recorded.*
- the notion that operators should avoid implying, that their CCTV system records everything, all the time. *[Obviously, it is not technically possible to record everything and there are MANY areas of the school, its classrooms and buildings, that are in CCTV blind spots.]*
- the differentiation between data usages. *[There is **actively-monitored data** – where a teacher actively views live data on a screen as part of the teacher's scheduled Playground Duty (PGD); **passively-monitored data** where a receptionist or dorm parent for example, might be required to occasionally monitor the live images from a camera to respond to a specific request – allowing entry through a gate or door, etc; **archived-for-retrospective-review-after-an-incident data** which as its name suggests is most likely never going to be looked at unless an incident occurs and requires the school to investigate – (this by the way, is by FAR the most common data use – probably 90% or more of the footage recorded will fall into this category); **archived for pedagogical or professional development review** purposes which is essentially the same as 'archived for retrospective review after an incident' except that the teacher who is recorded in the footage specifically wishes to review this footage later; and **recorded-for-production-purposes data** which is usually specific to either a lesson or assessment task that is being recorded for student instructional or assessment reasons.]*
- and finally, the fact that the school needs to publish its 'clear policy framework' so that all stakeholders (board, administration, staff, students, parents/carers and visitors) have no misconceptions about what the school is doing, why it is doing it and how it intends to use and store the data it captures. *[The following CCTV Policy Framework is the legal document that outlines the school's required, clear policy framework. This CCTV Policy Framework, needs to be available online (a PDF file accessible from the school's website) and provided in the Document Management Systems of all parents/carers within the school's LMS (Engage Parent Portal). Printed copies of the Policy need to be made available to any person who requests it in writing. A separate form: 'Request for a copy of The Kooralbyn International School's CCTV Policy Framework Form' should also be made available, to expedite any person's request of the document. This form should include the contact details of the person making the request and an address or email address that the school can use to despatch the document to within three (3) working days of receiving the written request.]*

The school's CCTV Policy Framework

(our clear policy framework) *v7.1*

Approving Authority:	TKIS School Board
Approval Date:	3 April 2022
Next Scheduled Review:	2026
Document URL:	https://www.tkis.qld.edu.au/PDF/CCTV_Policy_Full.pdf
Description:	This policy provides information on the use of surveillance, traffic optimisation and lesson capture technologies on The Kooralbyn International School property.

Introduction:
The school protects its students, its staff, its visitors and its assets to the best of its ability. Notwithstanding the many positive applications that the school plans to employ CCTV for (e.g. lesson capture and rescheduling for students who miss classes through illness or subject scheduling conflicts; professional development tools and pedagogical improvement; extended assessment evidence processes; general classroom behaviour management tools and assistance in helping to optimise traffic flow, workplace health & safety considerations and asset utilisation…the general rationale behind the use of CCTV as a surveillance medium comes from the notion that the visual presence of CCTV cameras provides a deterrence against inappropriate behaviour whilst hopefully reassuring students and staff that they are protected while on our campus and in our buildings and classrooms.

Management Responsibility:
Under the direct supervision of the school principal, the school's IT Department has the responsibility for the ongoing management of the CCTV system, including…

1. Controlling the operation of the CCTV system to ensure that it remains compliant with Government legislation (including Privacy, Copyright and WH&S legislation) and TKIS school policies;
2. Providing advice on the location of and utilities of cameras and storage mediums; and
3. Supporting the maintenance and upgrade of the cameras and network as required.
4. **Storage**: Ensuring that footage is stored for a period of up to 30 days. If no request has been made to view or access footage during this period, the media is overwritten.
5. **Access**: Ensuring that only authorised persons will have access to, and disclosure of, recorded images…and only for the purpose(s) that those persons are authorised. Ensuring that there is no access to or disclosure of images or data to third parties and in accordance with the school's CCTV policy framework matrix (see following).

1. The school's CCTV policy framework matrix

Type of CCTV footage	Who is recorded?	What is recorded?	What is produced?	Purpose?	Who can view it?	Authorised school staff	How long is it stored?
Outdoor surveillance raw footage	Those who approach or are on premises	24 hour a day, vision and IR only	Nothing. Raw footage archived only	General security and safety	Authorised school staff only	Principal Coordinators Reception PGD Staff IT Staff	30 days (incidents longer)
Outdoor main gate intercom raw footage	Anyone who happens to be in view	Vision and audio when activated	Nothing. Raw footage archived only	Security and access purposes	Authorised school staff only	Principal Coordinators Reception PGD Staff IT Staff	30-90 days (incidents longer)
Indoor Admin offices	Persons who enter and occupy offices	Video and audio 7:30AM to 4:30PM	Nothing. Raw footage archived only	Surveillance and child safety purposes	Authorised school staff only	Principal Coordinators PGD Staff IT Staff	30-90 days (incidents longer)
Indoor Dorm Buildings	Persons in corridors and stairwells	24 hour a day, vision and IR only	Nothing. Raw footage archived only	Surveillance and child safety purposes	Authorised school staff only	Principal Coordinators Dorm Staff IT Staff	30 days (incidents longer)
Indoor Classroom Whiteboards A	The teacher directing the lesson	Video and audio 8:30AM to 3:30PM	Nothing, but data available for review or editing.	Professional Development, Lesson efficacy	Authorised school staff and relevant teacher only	Principal Coordinators IT Staff Production	Raw: 30-90 days Produced footage: indefinitely
Indoor Classroom Whiteboards B	Data Capture or ECU on whiteboard only	Video and audio 9:00AM to 3:00PM	Nothing, but data available for review and editing.	Flipped Classroom or Distance Ed purposes	Authorised school staff, teacher and intended audience	Principal Coordinators IT Staff Production	Produced footage: Indefinitely
Indoor Classroom classes	Students in classroom	Video and audio 8:30AM to 3:30PM	Nothing. Raw footage archived only	Surveillance and child safety purposes	Authorised school staff only	Principal Coordinators IT Staff	30-90 days (incidents longer)
Inside and outside school buses	Traffic in front of bus and students and driver sitting in bus	Video and Audio when bus is in transit.	Nothing. Raw footage archived only	General security and safety	Authorised school staff only	Principal Coordinators IT Staff	30 days (incidents longer)

2. What is the process (if any) for an unauthorised person to request access to CCTV or similar footage recorded by the school?

Person making request	Request Format	Written Permissions required from	Appeals Process
Parent/Carer of child who appears in footage	School's CCTV Data Release Request Form	Every staff member and the parent/carers of every student identified in the footage	Not applicable
Parent/carer of child who does NOT appear in footage	Not applicable	Not applicable	Not applicable
Student who appears in the footage	School's CCTV Data Release Request Form	Every staff member and the parent/carers of every student identified in the footage	Not applicable
Student who does NOT appear in the footage	Not applicable	Not applicable	Not applicable
Staff Member who appears in the footage	School's CCTV Data Release Request Form	Every staff member and the parent/carers of every student identified in the footage	Not applicable
Staff Member who does NOT appear in the footage	Not applicable	Not applicable	Not applicable
Member of public	Not applicable	Not applicable	Not applicable
Member of Law Enforcement	School's CCTV Data Release Request Form	Every staff member and the parent/carers of every student identified in the footage unless…	A duly sworn warrant provided to the Principal

3. What information does the school's 'CCTV Data Release Request Form' require?

Your name (the name of person requesting CCTV data for non-commercial use):
Your contact details (address, email address, mobile):
The date, time and location of the recorded footage being requested:
Which CCTV camera (if know) recorded the footage you seek? (i.e. its location)
The reason you're requesting the footage (100 words or less):
Person or persons you believe will be identifiable in the footage:
Relationship of all such persons to yourself:
[NOTE: According to the school's CCTV Policy Framework, the Principal PLUS ALL PERSONS identifiable in CCTV footage (or their parents/carers in the case of students) need to provide their written permission to the applicant, before CCTV footage can be released to the applicant. Please attach written permissions – with contact information of the person(s) giving the permission – to this form.]
COSTS: CCTV footage that is approved for non-commercial release, will be dubbed to a single USB drive at a cost of forty dollars ($40.00) to be paid in advance, by the person requesting the CCTV data. If the CCTV camera or date and time of the recording is unknown, the school is likely to add a 'search charge' of $80 per hour. Please refer to admin for additional information.

4. Who are 'authorised school staff' and how are they selected?

Refer to 1.1 the Policy Framework matrix. Generally speaking, the school only authorises its Principal, Deputy Principal and essential IT or production staff to access the recorded CCTV footage. Obviously, staff who are employed to monitor 'live feeds from cameras', (e.g. teaching staff doing PGD - playground duty - by monitoring external CCTV cameras during morning teas and lunches; receptionists monitoring the main gate intercom; admin staff required to monitor students in Sickbays; Dorm Parents monitoring corridor and stairwell cameras after school, etc.,) are required to be able to view the live footage from the relevant cameras. Also, teachers who are leading a class lesson can request to review the recording of their own teaching performance for pedagogical purposes and teachers who are developing specific resources (flipped classroom, edited lesson highlights for students who missed a class, etc.,) can obtained restricted copies of their instruction which they can edit for students to observe later… such edited recordings should as much as possible, ensure that students in the class are not individually identifiable (camera angle from behind the student, face pixelated, names not mentioned, etc.)

5. How does a person obtain a copy of the school's CCTV Policy Framework?

The policy and additional background information is available from the school's website or can be downloaded directly from https://www.tkis.qld.edu.au/PDF/CCTV_Policy_Full.pdf

Persons who do not have access to the Internet can request a written copy of the policy by contacting the school on 5544 5500 during office hours and providing contact details for a copy to be posted to them.

6. What Signage does the school need to produce and display in order to meet its obligations under the various legislation?

In short, the school needs to make all reasonable effort to ensure that any person or persons considering entering school grounds is made aware of the fact that by entering school grounds, they are giving the school permission to record their activities using multi-level surveillance technologies and that such recordings are being made in accordance with Australian Privacy Principles, Child-Safe Standards and the school's WH&S and these CCTV Policy Framework guidelines. *(See Appendix A).*

7. What locations within the school are subject to CCTV and other forms of surveillance technology?

Public Areas: In locations where a person could reasonably expect that they are likely to be observed by another person, (e.g. by a staff member, a passer-by, etc.,) the school defines those locations as 'public areas' and a person's rights to privacy in those locations are effectively forfeit. For clarification purposes: In locations deemed 'Public Areas', the school is deemed to be within its rights, to record all observable activity. 'Public Areas' (for the purposes of this document) include…

- all open areas,
- car parks,
- entryways,
- classrooms and offices
- sickbays,
- stairwells,

- hallways,
- lobbies,
- eating areas and
- the outsides of buildings, etc.

Private Areas: Conversely, in locations where a person would have a reasonable expectation to privacy, such environments are deemed 'private areas' and within them, a person's rights to privacy must be fully observed at all times, regardless of any perceived security risk. The school will NOT place cameras or other recording technology devices of any kind in locations within the school deemed 'private areas'. 'Private Areas' (for the purposes of this document) include…

- inside toilet facilities,
- inside change rooms,
- inside boarding house bedrooms,
- inside showers or similar amenities,
- inside staff accommodation bedrooms, etc.

Out-of-bounds Areas: For clarification purposes, locations around the school and within its buildings that are deemed 'out-of-bounds' will be deemed acceptable for the placement of CCTV cameras and other forms of surveillance technology. 'Out-of-bounds Area' (for the purposes of this document include…

- alleyways between, behind and under certain buildings that are 'out-of-public-view',
- dangerous areas like steep hillsides and outside the school's fences and borders,
- the school's gyms,
- the school's swimming pool,
- the school's kitchens
- the school's chemical stores, etc.

8. For how long will recordings be maintained by the school?

In relation to recordings that ARE made on or within the school grounds, classrooms and buildings…

- Persons entering school grounds must be informed of the existence of multi-level surveillance technologies on campus and that entering the premises implies the person is giving tacit approval to the school to record their activities in accordance with the school's CCTV Policy Framework (see Item 6.)
- All multi-media recordings stored by the school are to be securely stored for legislative reasons for at least thirty (30) days in a network/system that is tamper-proof ensuring that data cannot be deleted or edited from its original source format. NOTE: The school is technically unable to guarantee the time frame that data will be stored, but the size of the storage space should be enough to store an average day's recordings for thirty (30) or more days. NOTE: There are no laws that demand private CCTV operators MUST keep recordings for any specific length of time. Thirty days is a recommendation only.
- Access to the school's multi-media recordings, (unless clearly identified within a separate teaching/learning context), is confined to the persons and within the situations those persons are authorised, within the school's CCTV Policy Framework.
- The data and recordings produced by the school's CCTV network can be used in conjunction with various surveillance technologies including Automatic Number Plate Recognition (ANPR); Traffic Flow Management; Facial Recognition and other Biometric Security systems.

Appendix A: Signage examples.

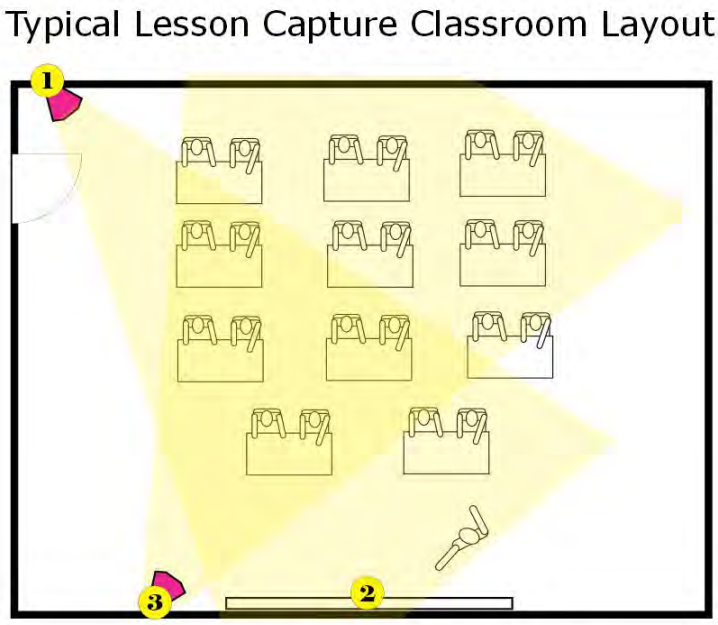
Welcome: You are entering a 'Child-Safe Environment'

The safety and security of our children and staff while on these premises, is our number one priority. For this reason, the school and its grounds are protected by multi-level surveillance technologies which may include audio-visual, heat signature and motion detection, time stamp; facial recognition and number plate recognition technologies.

Entering these grounds implies that you are giving tacit approval to the school to record your activities on campus using multi-level surveillance technologies. Call 5544 5500 for further information about obtaining a copy of the school's *CCTV Policy Framework*.

NOTE: All data and recordings made by the school are managed in accordance with Child-Safe Standards; Australian Privacy Principles; the school's WH&S and CCTV Policy Framework; the *Child Protection Reform Amendment Act 2017*; *Education and Care Services Act 2013*; *Child Protection (International Measures) Act 2003*; *Child Protection Act 1999*; *Information Privacy Act 2003*; *Surveillance Devices Act 2004*; *Privacy Act 1988*; *Copyright Act 1968* and *Copyright Amendment Act 2006.*

Appendix B: Typical Camera Layout in Classroom



1. Main Camera - POV Teacher and Whiteboard
2. Interactive Whiteboard or Digital Flatscreen recording
3. Reverse Angle Camera - (optional)

Appendix C

The: *should we put bars on windows?* quandary.

Safety and security management of an open-school campus like ours, means we're required to confront many complex issues. The most obvious, is the question of a person's rights to privacy versus their rights to an expectation of safety and well-being while on our campus. Another, often referred to as the 'bars on windows quandary', involves the question of whether personal safety should come at the price of having to turn one's home into a high-security fortress.

Most of the time, decisions relating to these types of questions are easy to resolve…a person's safety IS more important than their privacy. Safety in a workplace environment IS more important than the aesthetic appearance of that environment. In fact, according to *Maslow's Hierarchy of Needs*, after basic physiological needs (essential food and water, etc) **safety and security** are the primal human needs that surpass all others.

Sometimes however, situations are not always black and white. There are, for example, many physical locations on campus like toilets, change rooms, etc., where a person's expectations of privacy DO outweigh their concerns for safety and security. It's also fair to say, that most of us don't perceive our risks to personal safety warrant having bars on the windows or barbed wire on fences around a school like ours. Like many things in life, *the trick* is finding the right balance.

The various risk assessment and decision making matrices that TKIS uses in its Safety & Security Technology Management process include a support document (the school's CCTV Policy Framework) which provides various clarifying statements, one of which refers to the Privacy v. Security question and states: *"In locations where a person could expect that they are likely to be observed by another person, (e.g. by a staff member, a passer-by, etc.,) the school defines those locations as 'public areas' and a person's rights to privacy in those locations are effectively forfeit. Conversely, in locations where a person would have a reasonable expectation to privacy, (inside toilet facilities, change rooms and boarding house bedrooms for example), those environments are deemed 'private areas' and within them, a person's rights to privacy must be fully observed at all times, regardless of any perceived security risk."*

Further, in relation to recordings of audio-visual media, the support document states…

- Persons entering school grounds must be informed of the existence of multi-level surveillance technologies on campus and that entering the premises implies the person is giving tacit approval to the school to record their activities in accordance with the school's CCTV Policy Framework
- All multi-media recordings stored by the school are to be securely stored for approximately thirty (30) days in a network/system that is tamper-proof ensuring that data cannot be deleted or edited from its original source format.
- Access to the school's multi-media recordings, (unless clearly identified within a separate teaching/learning context), is confined to the persons and within the situations those persons are authorised, within the school's CCTV Policy Framework.
- The data and recordings produced by the school's CCTV network can be used in conjunction with various surveillance technologies including Automatic Number Plate Recognition (ANPR); Traffic Flow Management; Facial Recognition and other Biometric Security systems.

For the latest version of the school's CCTV Policy Framework, go to:
https://www.tkis.qld.edu.au/PDF/CCTV_Policy_Full.pdf