

SURVEILLANCE POLICY

Context

Christian Brothers' College St Kilda (CBC St Kilda) is a Catholic school for girls and boys in the Edmund Rice tradition, established in 1878. CBC St Kilda is committed to providing a caring, supportive and safe environment where every student has a place, a voice and their story is known. As a Catholic school in the Edmund Rice tradition, our Christian values are those expressed in the Touchstones of our governing body, Edmund Rice Education Australia (EREA): Liberating Education, Gospel Spirituality, Inclusive Community, Justice and Solidarity. The charism of Blessed Edmund Rice expressed through these touchstones, underpins our continued commitment to a safe and inclusive environment for all, providing a preferential option to those at the margins, to grow in empathy and to respond in faith and action.

Rationale

CBC St Kilda is committed to ethical behaviour that is aligned with the EREA Charter and Touchstones and complies with all relevant Commonwealth and State Government laws and regulations. The College is committed to providing a safe and secure environment for our students, staff and visitors and is also responsible for protecting our physical facilities, electronic systems, and managing its legal liabilities for surveillance devices.

This policy covers the College's obligations under the Surveillance Devices Act 1999 (Vic).

Policy Statement

This Policy covers the use of the following surveillance devices within College premises or which monitor facilities/or resources provided by the College:

- video and camera surveillance
- computer and other electronic surveillance
- tracking technology used for surveillance

It is College policy that:

- appropriate physical surveillance will be conducted for the purpose of:
 - providing safety and security within College premises or while using College facilities/resources
 - protecting students and staff and discharging duty of care obligations
 - preventing vandalism
 - assisting in the identification of criminal behaviour

- electronic and internet surveillance will be conducted for the purpose of:
 - identifying and stopping the flow of inappropriate or unlawful content, including viruses and spam, breaches of copyright and privacy legislation, discriminatory, harassing, or pornographic content
 - stopping other inappropriate or unwarranted use of the College's electronic resources
 - stopping other inappropriate or unwarranted use of the College's electronic resources
- existing students, staff, contractors and visitors will be given clear notice of any surveillance activities being undertaken except in the case of an investigation relating to suspected criminal activity
- surveillance activities conducted by the College are active 24 hours a day, 7 days a week, in order to enable the College to monitor and safeguard student wellbeing, OHS considerations for staff, students and visitors, and the protection of College assets
- new staff will be advised prior to commencing employment of the surveillance activities being undertaken by the College
- staff will be consulted prior to the implementation of new forms of surveillance equipment or procedures
- surveillance records are maintained in accordance with the College's Records Management policy and Privacy Program, and as required under this Policy.

Video and Camera Surveillance

Where the College determines that monitoring is required to maintain the safety or security of staff, students, visitors, or property as outlined in our Security (Building & Grounds) policy, the College may install security cameras inside or outside College buildings or otherwise on College premises.

The College operates security cameras as follows:

- outside College buildings, around the perimeter of College property, and otherwise on College grounds/premises; and
- areas where appropriate physical surveillance enables the College to monitor and safeguard student wellbeing, occupational health and safety, and duty of care considerations for staff, students and visitors, and the protection of College assets.

Signs indicating that the premises are under video and/or camera surveillance are clearly displayed and placed at all entrances to the College.

Computer and Other Electronic Surveillance

The College's Information & Communication (ICT) and Staff and Student Professional Boundaries policies set out the College's guidelines on appropriate and inappropriate use of College email and internet by staff and students. Computer surveillance allows monitoring of compliance with these guidelines, and enables prompt remedial action to protect students, staff, electronic resources and the College.

Computer surveillance may include:

- monitoring and maintaining internet usage history
- blocking and/or monitoring access to the internet or particular internet websites
- monitoring online/remote learning modules
- blocking and/or monitoring electronic messages transmitted using College facilities

Parents are supplied with software licences by the College to monitor their child's internet activity whilst at home. Parent use of this software is optional.

Staff, including new staff, are appropriately notified of computer or electronic surveillance. The College operates the following computer and/or electronic surveillance:

- external firewall
- pastoral care filtering system
- Catholic Education Melbourne internet filtering
- Microsoft email filtering
- electronic security locks reporting staff movement across campus buildings/rooms

Computer surveillance may take place even if the staff member or student is not onsite at work/school, provided that the surveillance relates to equipment, software or electronic resources paid for or provided by the College.

Tracking Surveillance

Tracking devices, such as the use of Global Positioning Satellite (GPS) technology may be used to monitor the location of staff and students for the purposes of maintaining the safety or security of staff, students, visitors or property. Tracking surveillance may be used on College vehicles and electronic devices. Tracking surveillance may be used on a device owned by staff or students which is used through College ICT systems. This will usually only be activated where the device is lost or misplaced, or the safety and security of the staff member or student is at risk.

Notification to Employees

Staff are made aware as part of their contractual obligations that surveillance is in operation at the College. The College will provide sufficient notice to staff of surveillance prior to commencement of employment.

The notice will indicate:

- the surveillance type (see 'Video and Camera Surveillance' and 'Computer and Other Electronic Surveillance' sections of this policy)
- how, when and where surveillance will be conducted (see 'Policy Statement' section of this policy).

Notice will not be provided where the employee has otherwise provided consent to the surveillance.

In cases where new forms of surveillance are engaged in by the College, parents and guardians will be advised before surveillance commences. However, it is the responsibility of the Principal to ensure the safety and security of the College, students, staff and visitors.

The College also publishes this policy on the College public website.

Prohibited Surveillance

It is not permitted by law to install, use, or maintain :

- video or audio surveillance to observe, listen to, record or monitor the activities or conversations of an employee in a toilet, washroom, change room or lactation room at the College a listening device to overhear, record, monitor or listen to a private conversation to which the College is not a party, without the express or implied consent of each party to the conversation;
- video surveillance to record or observe a private activity to which the College is not a party, without the express or implied consent of each party to the activity.

What is considered "private" will be determined against the College's child protection and duty of care obligations relating to students and staff.

Surveillance in the above circumstances may be permitted if it is done in accordance with a law of the Commonwealth or required by law enforcement in accordance with the Surveillance Devices Act 1999 (VIC).

Surveillance Records

Surveillance records are maintained by the College Network Manager, under the direction of the Principal, in accordance with the College's Records Management policy and Privacy Program.

Use, Communication and Publication of Protected Information

The College must ensure that any surveillance record made as a result of surveillance conducted under this policy is not used, published or disclosed unless that use, publication or disclosure is:

- made with the express or implicit consent of each party to the conversation or activity;
- no more than is reasonably necessary in the public interest or for the protection of the College's lawful interests; or
- in the course of legal proceedings.

Implementation

This policy is implemented through a combination of:

- staff training and supervision;
- effective record keeping procedures;
- effective incident notification procedures;
- effective communication procedures;
- initiation of corrective actions where necessary.

Discipline for Breach of Policy

Where a staff member breaches this policy, CBC St Kilda may take disciplinary action, including in the case of serious breaches, summary dismissal.

Student breaches of this policy will result in disciplinary action in accordance with College Student Behaviour Management Policy and procedures.

References

- EREA Charter
- Information & Communication (ICT) Policy
- Staff and Student Professional Boundaries Policy

Review

This policy will be reviewed December 2023, or earlier as part of EREA review of Comspace policies.