Workplace Surveillance Policy

Policy Classification		
Policy Number:	**Date of Origin:** February 2018	**Modification History:** Nil
Date of most recent review: Nil	**By Whom & Position:** Policy Review Committee	**Commencement Date:** 2018
Policy Audience: Oaklife	**Policy Status:** New	**Policy Review Date:** 2020
Policy Approval: This policy was approved by the Senior Leadership Team and Board February 2018.		
This policy supersedes all previous policies relating to matters contained herein.		

1.0 Rationale

1.1 The purpose of this Workplace Surveillance Policy is to describe surveillance at Oakhill College.
1.2 Oakhill College surveillance may occur by means of camera, computer, and tracking devices, and requires that all stakeholders including but not limited to staff, students, parents, volunteers, service personnel and visitors, be notified as to the nature of that surveillance.
1.3 This Workplace Surveillance Policy constitutes the provision of notice to all stakeholders of Oakhill College's workplace surveillance under the Workplace surveillance Act 2005 (NSW).

2.0 Guiding Principles

2.1 This Policy applies to all current employees, contractors, and consultants who have access to any College premises, equipment, or systems, including IT Resources and Networks.
2.2 The Workplace Surveillance Act 2005 (NSW) (the Act) regulates what surveillance, including computer surveillance, can be carried out by an employer while an employee is at work for the employer.
2.3 The College may take disciplinary action, up to and including termination of employment, for any breach of this Policy.
2.4 This Policy should be read in conjunction with relevant College policies, including:
Code of Conduct;
Digital Information Security Policy;
IT Acceptable Use of Resources Policy
Privacy Policy

3.0 Policy

3.1 Surveillance Consisting of Monitoring

3.1.1 The College carries out Surveillance in the form of monitoring to ensure:
a. the health, safety and welfare of College Employees, students and visitors, for example, by installing fixed cameras throughout the campus;
b. the integrity, security and service delivery of its systems and Networks; and
c. compliance with its legal obligations, including reporting obligations.

3.1.2 In the course of carrying out Monitoring, the College collects, creates and stores records and information (including logs, images, backups, and archives) using any one or more of the following methods:
a. Telephone Monitoring - the College phone system is able to Monitor input and output of telephones (both fixed line and mobile) devices provided by the College for use by Employees. These may be Monitored and may be accessed for administrative purposes;
b. Camera Monitoring - the College has installed fixed security cameras throughout the campus, both inside and outside of buildings and other facilities. These cameras (including any casings) are not covered or hidden, and Monitor activities on an ongoing and continuous basis;
c. Computer Monitoring - the College conducts ongoing Monitoring of the following:
i. College email accounts, and emails sent or received using a College email account or a College server;
ii. internet usage, including browsing history, content downloads and uploads, video and audio file access, and any data input using the College IT Resources; and
iii. access (including logons) to, and all activity on, the College IT Resources including computer hard drives and servers, and any files stored on IT Resources;
d. Tracking Monitoring - the College may monitor or track the location or movement of individual Employees. However, it does provide and make available for use by Employees equipment and devices that have functionality to monitor and record their geographical location or movement, for example:
i. mobile telephones, hand-held radios, laptops, tablets and similar devices;

ii. access cards into College buildings;
iii. College-owned vehicles with global positioning systems installed;
iv. fuel cards issued for College-owned vehicles; and
v. wired and wireless data point connections installed in College buildings.

3.1.3 In carrying out Monitoring, the College records and stores information and creates records (including reports) in relation to the following that are Surveillance Information and Surveillance Records for the purposes of the Act:

a. movements within a Workplace;
b. access to secure College facilities (buildings and locations within buildings);
c. connection of devices (whether or not owned by the College) to College IT Resources and the Network. This includes logging access at specified wired and wireless data points;
d. emails sent or received using College email accounts or through College servers, storage volumes, download volumes, browsing or downloading history on College IT Resources; and
e. any information or data created or managed on, downloaded to and stored on College IT Resources, servers and other devices that the College supplies or otherwise makes available for use, including College email.

3.2 Surveillance and Surveillance Information and Records

3.2.1 The College may from time to time:

a. conduct Surveillance, including Surveillance of individual Employees; or
b. access, use or disclose information or records obtained in the course of Monitoring for Surveillance in relation to individual Employees.

3.2.2 The College may use or disclose Surveillance Information or Surveillance Records for purposes authorised under the Act and in accordance with the procedures set out in Section 4 of this Policy. These specifically include:

a. for legitimate purposes related to the employment of Employees;
b. for the legitimate business activities or functions of the College, including internal inquiries and investigations of alleged unlawful activities or activities that are alleged to be in breach of any College rule, policy or code of conduct or in breach of a person's duties to the College as its Employee;
c. for use or disclosure in any legal proceedings (including an inquiry by the Independent Commission Against Corruption or the NSW Ombudsman) to which the College is a party or is directly involved;
d. disclosure to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
e. where otherwise required or authorised by law to do so (for example, if the College is required to comply with a search warrant or subpoena);
f. where the College considers this is reasonably necessary to avert a serious and imminent threat of:
    i. serious violence to a person;
    ii. damage to property (including disruption to the College's business, systems or operations).

3.3 Prohibited Surveillance

3.3.1 The College will not carry out and does not condone any of the following which are prohibited under the Act:

a. Surveillance of Employees in a change room, toilet facility or shower or other bathing facility in the Workplace;
b. Surveillance of Employees using work Surveillance devices when Employees are not at work, except as permitted under the Act and this Policy; and
c. Blocking emails or internet access of an employee except as permitted under the Act.

4 Procedures for Conducting Surveillance

4.1 Notice Requirements

4.1.1 This Policy is a formal notice to Employees that the College does the following in accordance with this Policy:

a. it conducts Surveillance in the form of Monitoring in the Workplace;
b. where authorised under the Act or this Policy, it conducts Workplace Surveillance other than Monitoring; and
c. it creates, accesses, uses and discloses information or records in relation to Surveillance, including as part of Monitoring.

4.1.2 The College also provides notice to Employees about Surveillance (including Monitoring) in other formats as follows:
a. in the case of Monitoring by cameras, by means of physical signage at the entrances to or within campus grounds;
b. by signed acknowledgement in an employment contract;
c. by means of the Staff Handbook
d. for new methods of Monitoring, specific written notice to all Employees (which may be given by email) at least 14 days before that routine Monitoring commences.

4.1.3 For approved Surveillance the College must send a written notice authorised by either the Principal or Deputy Principal, and must specify:
a. the type of Surveillance or new form of Monitoring to be carried out;
b. how it will be carried out;
c. when it will start;
d. whether it will be continuous or intermittent; and
e. whether it will be for a specified limited period or ongoing.

4.1.4 Written notice to an employee under clause (4.1.3) will not be provided:
a. where there is a risk of disclosure of the identity, or exposure to reprisals, of a person who has made a public interest disclosure under the College's policy relating to public interest disclosures;
b. where Surveillance information or records are aggregated in a format that does not identify specific individuals, including Employees, for example, for operational support reasons.

4.2 Blocking of Email or Internet Use

4.2.1 The Act prohibits the College from blocking an employee from accessing the internet or sending or receiving emails unless:
a. the College acts in accordance with its policies relating to email or internet access that have been notified to the employee in advance in such a way that it is reasonable to assume the employee is aware of and understands the relevant policy; and
b. if the College intends to prevent delivery of an email, the College gives the employee notice (which can be by email) that delivery of the email will be blocked.

4.2.2 The College is not required to give notice under clause (6.3.1b) if:
a. the College regards the content of the website or email, including any attachment, as menacing, harassing or offensive, for example, pornographic, gambling or terrorist websites;
b. the email is or contains a commercial electronic message, as defined in the Spam Act 2003 (Commonwealth);
c. the content or attachments of the email would or might result in unauthorised interference with, damage to or operations of an IT Resource (including any program run or data stored on any IT Resource);
d. the sender of the email has been identified as having previously sent malicious content to the organisation;
e. the College is not aware (and cannot reasonably be expected to be aware) of whether an employee has sent that email or of the identity of the employee who has sent that email.

4.3 Authorizing Surveillance

4.3.1 All stakeholders are prohibited from conducting any form of Workplace Surveillance or from accessing Surveillance Records or Surveillance Information, except the following Employees who are only authorised for the purposes of performing their designated duties as Employees:
a. Employees (including those within the IT Department) whose normal duties include routine back up or restoration of data, conduct of audits, review of web filtering, email filtering, document retrieval or logs, or other activities relating to the College's systems, including IT Resources and Networks;

b. Employees (including those in the IT and the Maintenance Department) whose normal duties include review of camera footage and of building access (including use of building access devices); or
c. Employees who are specifically authorised by the Principal to conduct Surveillance or to access Surveillance Information or Surveillance Records.

4.3.2 Requests to authorise Surveillance that go beyond Monitoring, or to authorise access to Surveillance Information or Surveillance Records by persons other than those listed in clause (4.3.1), may only be made by one or more of the following persons and only for a purpose specified in clause (3.2.2):
a. the Principal;
b. the Deputy Principal;

4.3.3 Only the following persons can approve a request (except where they are the subject of the request):
a. the Principal;
b. the Deputy Principal;

4.3.4 For the avoidance of doubt, Surveillance requests made under clause (4.3.2) will only be approved if the persons authorised to grant approval are reasonably satisfied that:
a. the request is for a purpose specified in clause (3.2.2);
b. if the request is for a purpose specified in clause (3.2.2b):
   i. there is no less intrusive alternative, reasonably available, in the circumstances, including, but not limited to, any need for urgency;
   ii. the proposed method and length of Surveillance or access to information and records is reasonable and appropriate in the circumstances; and
   iii. reasonable precautions will be taken to ensure the integrity and security of data, including compliance with the College's Privacy Policy.

5 Supporting Documents, Procedures and Guidelines

Nil

6 Policy Review

The College, via the Principal is to ensure that this Policy is monitored and revised to ensure that it delivers the requirements of the Workplace Surveillance Act 2005.

7 Explanatory Notes and Definitions

7.1 Important provisions that employers should be aware of are contained in sections 9 to 18 of the Act. A brief outline is provided below:

- Computer surveillance of an employee must not be carried out unless the employer has a policy on computer surveillance and the surveillance is carried out in accordance with that policy: section 12(a) of the Act
- Employees must be notified in advance of the policy: section 12(b)
- The surveillance must not commence without written notice to the employee and at least 14 days' notice given (unless a lesser period is agreed between the parties): section 10(1) and (2)
- For future employees this requirement will be met if the notice is given before the employee starts work: section 10(3). For example: a copy of the policy is given to the employee with their contract of employment
- The notice must specify the kind of surveillance, when it will commence, whether it is continuous or intermittent and ongoing: section 10(4)
- The notice may be given by email: section 10(5)
- Employers must not prevent delivery of an email or access to a website unless the employer is acting in accordance with a policy notified in advance to employees: section 17(1)(a)
- Employers must give the employee a prevented delivery notice as soon as practicable (by email or otherwise) that delivery of an email has been prevented: section 17(1)(b)
- A prevented delivery notice is not required where the employer believes that:
  - The email was spam

- The email would cause damage to the computer or network
- The email would be regarded as menacing, harassing or offensive
- The employer was not aware of the identity of the employee: section 17(2)

7.2 Definitions

The Act does not separately distinguish the terms "Surveillance" and "Monitoring", and the term "Monitoring" is defined separately in this Policy to provide clarity. However, it is still a form of "Surveillance" as defined in the Act. For the purposes of this Policy:

a. "Act" means the Workplace Surveillance Act 2005 (NSW);
b. "at work" includes when the employee is at an Oakhill College Workplace whether or not he or she is actually performing work at the time, or at any other place while performing work for the College or utilising College resources or services;
c. "Employee" means current employees, contractors, and consultants who have access to any University premises, equipment, or systems, including IT Resources, adjuncts, conjoints and students;
d. "IT Resources" means systems, software, hardware, and other forms of technology, communication or other similar services owned or managed by the University;
e. "Malicious Content" means content of a profane or inappropriate manner including, but not limited to:
    i. pornography;
    ii. sexual content;
    iii. defamatory content;
    iv. content that harasses, threatens or bullies a person;
    v. racist content; and
    vi. violent content;
f. "Monitoring" is a form of Surveillance, and means the collection or storage of information, or the creation of records, in a routine and passive manner. It also includes routine review of that information or those records to ensure the integrity, security and service delivery of the University's systems, including IT Resources and Networks. However, and for the avoidance of doubt, Monitoring does not involve actively investigating or keeping track of an individual or his or her activities.
g. "Network" means network hardware and the services operating on the hardware or utilising the hardware to perform tasks, whether wired or wireless.
h. "Policy" means this Workplace Surveillance Policy and includes any Schedules or attachments;
i. "Surveillance" of an Employee means surveillance of an Employee by any of the following means:
j. camera surveillance which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place;
k. computer surveillance which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of internet websites);
l. tracking surveillance, which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a global positioning system tracking device);
m. "Surveillance Information" means information obtained, recorded, monitored or observed as a consequence of Surveillance of an Employee;
n. "Surveillance Record" means a record or report of Surveillance Information;
o. "College" means Oakhill College
p. "Workplace" means any College premises, or any other place, where employees work, or any part of such premises or place.

For the avoidance of doubt words or terms used in this Policy have the same meanings given to them in the Act.