Portland Secondary College

Portable Storage Device Security Policy

PURPOSE

This policy defines the rules for The Department of Education and Training, and all Departmental information on portable devices (PSDs) where the information is classified as sensitive or protected in the Department's Information Security Classification Scheme. This classification is used when compromise of the information could cause damage to the Victorian Government, students, staff, commercial entities or members of the public and includes the access of staff and students' personal details. The purpose is to make sure that schools manage and share information appropriately and securely in order to meet information security obligations and to appropriately protect staff, students and their families.

SCOPE

This policy applies to all users of Portable Storage Devices within the Department.

DEFINITIONS

Portable Storage Devices includes laptops, netbooks, tablets, mobile phone and smart devices, thumb drives, flash drives, external hard drives and any devices with built-in accessible storage.

Bring Your Own Devices are considered portable storage devices and as such are considered in the scope for this policy.

Personal Information is recorded information or opinion about an identifiable individual. It can be almost any information linked to an individual, including name, address, sex, age financial details, marital status, education or employment history.

Sensitive information includes but is not limited to student information including name, address and date of birth; student academic records, progress reports, assignments and assessments; student health and medical information; student information pertaining to family circumstances; student class photographs and images; parents' names, address, phone number, email address and custody instructions; teachers' personal information; parents' banking and credit card information; school financial information; tendering and procurement documents, vendor invoices, contacts and account payable and receivables.

POLICY

Principals must establish appropriate practices to protect critical and sensitive information.

These include:

- encouraging staff to complete the Information Security of School Staff eLearning Module on an annual basis
- including the completion of this module as part of the new staff Induction Program
- identifying who has access to sensitive information – limited to ES Staff and Teaching staff on Compass and Admin staff on CASES21.
- revoking access to Compass and CASES21 in a timely manner when required
- ensuring all staff know what constitutes an Information security alert and how to report concerns to the Principal Class
- identifying critical and sensitive information and storing it in approved and trusted locations

- protecting Information and ICT equipment by housing all ICT infrastructure and personal computers (when not in use), in a locked and secured location with restricted access.
- not sharing or leaving devices or passwords where they can be easily accessed by others
- identifying and publishing the names of students who have not given consent for their photograph or image to be taken and/or used
- inviting parents once a year to check the information stored about themselves and their student once every 12 months
- ensuring casual relief staff passwords are changed regularly
- ensuring students do not use generic logins
- ensuring the ICT department work with staff to ensure the devices have encryption software installed and enabled; are protected by a password; be configured to lock automatically after a defined number of consecutive failed login attempts; be configured to require re-entry of the password, passcode or PIN after a period of inactivity; have up to date software installed to protect against viruses, trojans and other forms of malware; have a firewall installed and turned on securely in order to restrict data traffic into and out of the device
- encouraging staff to protect their devices form loss and theft by taking normal precautions
- Regularly communicating and reminding staff about necessary security measures

When storing Sensitive Departmental information on a PSD, staff must make sure confidential information is protected and consider the risks of unauthorised access to the data.

Staff are reminded:

- To not lend their device to students to use
- To minimise the window they are working in if students approach
- To lockdown device if leaving it unattended
- To never enter a staff username/password into a student's device
- To take care not to access other programs such as email when using the device connected to a projector/TV
- To ensure that passwords comply with DET regulations (minimum 8 characters, minimum one capital and minimum one symbol)
- To not access Compass or like program on a shared device

It is the responsibility of the ICT Manager to remind staff of the above guidelines regularly at the beginning of each year.

The ICT Manager will regularly review network configuration and anti-virus and patching arrangements and ensure that the College's internet provider arrangement meets the requirements of DET standards. The ICT Manager will also ensure that all relevant Privacy Impact Assessments are completed. The ICT Manager will be responsible for posting an item in the School's newsletter each year which outlines the collection and storage of protected and sensitive information.

It is the responsibility of the Office Manager to ensure consent for the taking and publication of student photos is gathered each year and then publishing the names of students who have not been given consent so all staff are aware.

All requests to access personal, private, protected or sensitive information of students and staff must be directed to the Principal.

ADDITIONAL POLICIES, GUIDELINES AND RESOURCES

- DET Information Security – InfoSafe Policy
- DET Photographing, Filming and Recording Student Policy
- PSC Photographing, Filming and Recording Student Policy
- DET Photographing, Filming and Recording Staff and Other Adults Policy
- DET Privacy and Information Sharing
- Schools Privacy Policy
- DET Records Management – School Records

REQUIRED METHOD OF COMMUNICATION

- Portland Secondary College Council
- Staff induction process
- School Website

REVIEW CYCLE AND EVALUATION

DATE	VERSION	RATIFIED BY	NEXT REVIEW
Aug 2020	1	Portland Secondary College	Aug 2023