GUIDELINE: Capturing and Storing Images of Students

1. PURPOSE

The purpose of this guideline is to outline how digital images and recordings of students should be captured and stored in a manner which aligns with the Catholic Education Archdiocese of Brisbane Code of Conduct.

The Code of Conduct states that the responsibility of the employee is to:

- not use a personal device (personal camera, personal mobile phone, or personal video recorder) to take, record, or store any student information (e.g., phone number, email address, etc.), recordings or images, unless they have obtained the prior approval of the parents/carers and their Principal and there is a reasonably justifiable and appropriate educational context. Any digital material captured should be transferred to a BCE resource as soon as reasonably possible and permanently deleted from the personal device.
- only use a BCE device (e.g., iPad, phone, camera, etc.) to record, photograph or video a student if there is an appropriate and professional educational reason.

Refer to the Media Consent procedure for any images of students used for community publication and planning staff activities (see Spire).

2. GUIDELINE

Appropriate capture of images

Prior to capturing any images of students, an employee should ensure they are using a BCE device i.e., classroom iPad or school camera.

During school events i.e., excursions, swimming carnivals or camps, the school should ensure they allocate responsibility for capturing images of the event to an appropriate school employee. The school should ensure that students, other employees, parents, and volunteers are aware of who the allocated school employee is.

If students, parents, employees, or volunteers are seen capturing images/recordings during the event, the school should ask them to discontinue, delete the images/recordings and, if required, referred to the allocated school employee.

Appropriate storage location

The most appropriate digital storage location is each employee's school's Staff Drive on the School Portal (SharePoint) and Parent Portal. A school should have a folder structure located in the staff section of the School Portal whereby employees can access a common space to upload photos.

Method	Risk	Mitigation
Camera roll on a personal device (or similar)	High	Avoid use of a personal device. If unavoidable, seek appropriate consent from parents/carers and their Principal. Any digital material captured should be transferred to school or parent portal as soon as

Method	Risk	Mitigation
		reasonably possible and permanently deleted from the device. Ensure a pin code is set on the device.
OneDrive app on a personal device	High	Although an employee's OneDrive is a secure location, it is still considered unsecured on a personal device. To reduce risk, it is recommended to enable the pin code.
Any school device	Moderate	If needing to retain images stored to the camera roll of any school device, ensure they are moved to a media folder location in a school portal. Once uploaded, delete all images from a staff device. An employee may choose to temporarily store images in the work OneDrive. Images stored in an employee's OneDrive should also be moved to the staff portal as soon as reasonably possible, due to risks associated with sharing permissions.
School Portal/Parent Portal/BCE Connect	Low	Ensure that all original images are deleted from the device as soon as reasonably possible.

Personal device

When an employee has obtained appropriate consent, the content should be relocated to an appropriate BCE digital place of storage as soon as possible. Once moved, the content should be deleted from the employee's personal device immediately.

OneDrive on my personal device

An employee can choose to download the OneDrive app on their personal device and log in using their BCE username and password. The OneDrive app will allow an employee to take photos and videos directly on their personal device. However, the content will save to their OneDrive and not onto their device's camera roll.

It is recommended that the content is transferred to the school portal as soon as reasonably possible and removed from their OneDrive app. The content located in the app can still be accessed if the employee's device is compromised. It is recommended that employees enable the pin code security setting.

Photos in BCE Connect/Parent Portal

When using the blog feature, employees may use their personal device or work device when taking photos or videos in the BCE Connect app. These photos or videos should not be saved to the device camera roll. Instead, the content should be uploaded directly to the blog post.

School Owned Device

An employee may also choose to use their BCE OneDrive account to store images. However, it is recommended that the content is transferred to the school portal as soon as reasonably possible.

Employees who have been supplied with a laptop, staff iPad, Android and/or Apple phone may request to have the OneDrive App loaded onto their device. Given the device is school

owned, it is also appropriate to use the camera roll feature on the device for a reasonably justifiable and appropriate educational reason. A risk is present if the device is lost or accessed by someone outside of the school. The content captured on the device should be uploaded to the school portal as soon as reasonably possible and deleted from the device's camera roll or OneDrive. It is recommended to enable the pin code security setting.

School camera or video camera

When taking photos, or video on a school camera or video camera these images should be saved to the local storage card (SD card or similar). These images and videos should be uploaded to the school portal and then deleted from the device storage as soon as reasonably possible.

Social media/public websites/school newsletters

All photos of students uploaded to public platform should be checked to ensure public media consent has been given prior to posting the photo. Media consent status for each student can be found in eMinerva.