

# Software and Online Services Policy

## PURPOSE

This policy outlines measures staff must take to support students to engage with digital technology in a safe and responsible way.

Schools must:

Educate staff and students on the importance of maintaining privacy when using software and other online services for learning and teaching.

### **Authorised software and online services that meets the following conditions:**

- The software is used in accordance with licence terms
- The software has been tested by an authorised ICT Officer to ensure functionality and security of ICT Facilities
- The software has been installed by an authorised ICT Officer or the installation of the software has been authorised by an ICT Officer
- That privacy impact assessment (PIA) has been filled out and been approved

### **Unauthorised software and online services is any software that:**

- Is used in breach of software licence agreements
- Has not been tested by an authorised ICT Officer
- Is not installed by an authorised ICT Officer or installation has not been authorised by an ICT Officer.
- Has not done a privacy impact assessment (PIA) and has not been approved

### **Unlicensed software is all software used outside of the licence**

- Agreement that accompanies the software
- The use of unlicensed software on Warragul Regional College ICT facilities is strictly prohibited, and any instance immediately renders the software unauthorised
- The installation and use of unlicensed software cannot be authorised by any person
- The software may not be installed or used until the conditions of the licence have been met
- Any software installed or used in violation of licence terms shall be deemed unauthorised software and will be in breach of this policy.

### **When a privacy impact assessment (PIA) is required**

When schools are considering using an online service or application that handles personal information they must:

1. Obtain agreement to do so from the school principal or leadership team. This can be done via email or a meeting.
2. Conduct an assessment to identify any privacy and security risks, and document what actions are required to mitigate these.
3. Consider whether consent for use of the service is required, and if so, whether opt-in or opt-out consent is most appropriate for the specific situation.
4. Ensure parents are adequately informed about the use of the online service.

## FURTHER INFORMATION AND RESOURCES

Refer to Cybersafety and Responsible Use of Digital Technologies

<https://www2.education.vic.gov.au/pal/cybersafety/policy>

Refer to Privacy and Information Sharing

<https://www2.education.vic.gov.au/pal/privacy-information-sharing/policy>

<https://www2.education.vic.gov.au/pal/privacy-information-sharing/guidance/privacy-impact-assessments>