

# School Policy

## Cyber Safety

---

### Rationale

Avenues Education endeavours to meet all its responsibilities as outlined in the school policies and relevant legislation for the physical and emotional safety of the students attending its school and all employees. This includes the need to establish and maintain the cybersafety of the school environment.

This policy has been developed as part of the Avenues Education cybersafety programme, and is designed to:

- Educate Avenues Education staff about cybersafety issues.
- Provide guidance regarding the safe and responsible use of ICT at Avenues Education.
- Outline the nature of possible consequences associated with breaches of the Avenues Education cybersafety policy, which may undermine the safety of the school's environment.

Important terms used in this document:

- a) The abbreviation 'ICT' refers to the term 'Information and Communication Technologies'.
- b) 'Cybersafety' refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones.
- c) 'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below.
- d) The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use
- e) 'Objectionable' in this context means material which is illegal, and can include such material as images of child sexual abuse, extreme violence, and extreme cruelty. Some material such as pornography (of a type similar to that which can be legally purchased from video or magazine outlets), may be classified as 'restricted'. Although the material itself may not be illegal, it is illegal to supply restricted material to people under a certain age.

Avenues Education acknowledges:

- The Internet, and ICT play an increasingly important role in the learning of students and in the administration of education services
- The need for establishment and implementation of a cybersafety policy and cybersafety use agreements for Avenues Education staff, students and parents/carers
- The school Cybersafety Policy contributes to the provision of a safe learning environment which fosters students' emotional, physical and social development
- The school Cybersafety Policy contributes to the maintenance of a safe work environment
- The school Cybersafety Policy assists Avenues Education to meet its obligations to deliver curriculum which promotes the health of students, nurtures students' well-being, and keeps students safe from harm. The policy document and related use agreements are not intended to be exhaustive documents containing all relevant rights and obligations that may exist in legislation to regulate use, storage and dissemination of information.
- Some online activities are illegal and will be reported to the police.

## Objectives

This policy will assist Avenues Education to:

- Meet its legal obligations as outlined in the previous section
- Provide guidance to Avenues Education staff, students and parents / carers, regarding the safe and responsible use of ICT at Avenues Education
- Educate members of the Avenues Education community regarding the safe and responsible use of ICT.

## Documentation in place

Student Code of Conduct

ICT Use Policy

Use of ICT Agreements

Induction Lists

Cyberbullying Incident Reporting Form

Guidelines for Teachers Dealing with Cyberbullying

Cybersafety Policy

Anti-Bullying Policy

## Definition of Cybersafety

Avenues Education uses the following definition of Cybersafety:

- The safe and responsible operation/use, at any time, on or off the school site, and by any person, of the school's Internet facilities, network, and associated ICT equipment/ devices, such as computers and laptops, digital cameras, mobile phones, and other devices noted above
- The safe and responsible use by anyone, of any privately-owned ICT equipment/devices on the school site, or at a school-related activity.

## Cybersafety Practices

At Avenues Education we:

- Provide a filtered internet service
- Provide supervision and direction in online activities and when students are using digital technologies for learning
- Support students in developing digital literacy skills
- Use mobile technologies for educational purposes
- Provide support to parents/carers to understand this agreement.
- Utilise a Security systems which represent good practice including:
  - Updated anti-virus software
  - Updated firewall software or hardware
  - Updated anti-spyware software
  - Regularly patched operating systems
  - Secure storage of ICT equipment/devices

### Permitted use

Use of the Avenues Education computer network, Internet access facilities, computers and other school-owned ICT equipment/devices (including mobile phones) on or off the school site, is restricted to:

- Avenues Education staff
- Parents / Carers of enrolled students, and/or other visitors
- Persons contracted to carry out work at the school and at the discretion of the Principal such as trades people or technicians.
- School-related activities.
- Personal usage by Avenues Education staff (such as professional development) which is appropriate to the school learning environment and is of a reasonable amount.

## **Parents/carers consent for students to use ICT**

Parents/carers consent for students to use ICT at Avenues Education by signing an ICT Consent Form.

## **Privately-owned/leased ICT equipment/devices**

Use of privately-owned ICT equipment/devices (including mobile phones) at the school or any school-related activity is restricted to activities which are appropriate to the school learning environment. This includes storage of any images or material on such devices.

## **Appropriateness of use and content to Avenues Education learning environment**

The Principal will provide guidelines as to what is considered appropriate to the school learning environment, including the taking of photographs or video.

## **User accounts and passwords**

Access to the school's computer network, computers, and Internet access facilities, requires a password protected personal user account. It is important that passwords are strong. The password must comply with DET Password Policy:

- Uses a combination of upper and lower case letters, numbers and other characters.
- Is a minimum of 8 characters in length.
- Is changed regularly.

## **Filtering and monitoring**

The school may utilize filtering and/or monitoring software where appropriate, to restrict access to certain websites and data, including email.

The school reserves the right to monitor, access, and review all use of school-owned ICT equipment/devices including personal emails sent and received using the school's computers and/or network facilities, either during or outside school hours.

## **Ownership of electronic files or data**

Any electronic data or files created or modified for the purpose of completing work on behalf of Avenues Education on any ICT, regardless of who owns the ICT, are the property of Avenues Education.

## **Auditing**

Avenues Education may from time to time, at its discretion, conduct an audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices.

## **Performing work-related duties at home using privately-owned equipment/devices**

Where it is necessary for Avenues Education staff to regularly perform school-related duties (e.g. school accounts or official correspondence) on privately-owned ICT equipment/devices at home, this work should be authorized by the Leadership Team.

## **Inappropriate activities/material**

Avenues Education will take all reasonable steps to filter or screen all material accessed using the school's network or Internet access facilities. However when using a global information system such as the Internet, it may not always be possible for the school to restrict access to all such material. This may include material which is inappropriate in the school learning environment, dangerous, or objectionable.

While using the Avenues Education network, Internet access facilities or ICT equipment/devices, or using any privately-owned ICT equipment/devices at the school or at any school-related activity, no person may:

- Initiate access to, or have involvement with, inappropriate, dangerous, illegal or objectionable material or activities.
- Save or distribute such material by copying, storing or printing.

### **Accidental access to inappropriate material**

In the event of accidental access to any inappropriate material by a parent / caregiver, or other visitor, a member of the Avenues Education staff should be consulted.

Where the material is clearly of a more serious nature, or appears to be illegal, users should:

- Remove the material from view (by closing or minimising the window, turning off the monitor, or shutting down the device).
- Report the incident immediately to the Avenues Education Principal.

### **By Avenues Education staff**

In the event of accidental access of inappropriate material at the lower range of seriousness (e.g.Spam), Avenues Education staff should delete the material.

If the nature of such material is somewhat more serious, (e.g. spam containing inappropriate but not illegal images), delete it and notify the Principal.

In the event of accidental access of inappropriate material clearly of a much more serious nature, or of material, which appears to be illegal, users, should:

- Remove the material from view (by closing or minimising the window, or turning off the monitor).
- Report the incident immediately to the Principal who will take such further action as may be required under this policy.

### **Unauthorized software or hardware**

Only legitimately acquired software may be used and only in accordance with licensing conditions. Authorization from Principal must be gained before any attempts to download, install, connect or utilize any unauthorized software or hardware onto or with any Avenues Education ICT equipment/ devices. This includes use of such technologies as Bluetooth, infrared, and wireless, and any similar technologies which have been, or may be developed. Any user seeking authorization should speak with the Principal.

### **Student's use of the Internet**

Students will be actively supervised by Avenues Education staff, or by someone who has signed an Avenues Education cybersafety use agreement when accessing the Internet on the school's site or at any school-related activity.

### **Confidentiality and Privacy**

The principles of confidentiality and privacy extend to accessing or inadvertently viewing information about personnel, or students and their families, which is stored on the school's network or any device.

Privacy laws are such that Avenues Education staff should seek advice from school management regarding matters such as the collection and/or display/publication of images (such as personal images of students or adults), as well as text (such as students' personal writing).

Department of Education guidelines will be followed regarding issues of privacy, safety and copyright associated with the online publication of students' personal details or work

### **Posting material**

All material submitted for publication on the school Internet/ Intranet site should be appropriate to the school's learning environment.

Such material can be posted only by those given the authority to do so by the school management.

The school management should be consulted regarding links to appropriate websites being placed on the school's Internet/ Intranet (or browser homepages) to provide quick access to particular sites.

Involvement as a representative of Avenues Education with any non-school website must be with the approval of the school management.

### **Cybersafety training**

Where personnel who supervise student's use of ICT indicate they require additional training/professional development in order to safely carry out their duties, the Principal will consult with agencies which provide such training.

**Breaches of this policy**

Breaches of this policy can undermine the values of the school and the safety of the learning environment. Any breach which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or the use of ICT to facilitate anti-social behaviour such as harassment), may constitute serious misconduct. The Principal will respond to any breach of the use agreement in an appropriate manner. If there is a suspected breach of this policy involving privately-owned ICT on the school site or at a school-related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s).

If an incident is being investigated in which use of school ICT by any person who does not have a signed use agreement with the school includes some level of involvement by Avenues Education staff, the extent of the Avenues Education staff responsibility will be assessed by the Principal and/or Leadership Team.

Any breach concerning involvement with material which is deemed 'age-restricted', or 'objectionable' under the Classification Act 1995, is a very serious matter. In such situations, it may be necessary to involve the police in addition to any response made by the school as a result of its investigation.

**Review of Policy**

This policy will be reviewed as part of the school's three-year review cycle.

**Ratification**

This policy was adopted at the School Council meeting held at Box Hill on 14 August 2017

Signed: .....  
School Council President

Signed: .....  
Principal