# DANDENONG HIGH SCHOOL

# STAFF SOCIAL MEDIA POLICY

---

## Preamble

All members of the school community, staff, students and parents are increasingly using digital technologies for professional purposes (i.e. teaching and learning) and personal purposes (i.e. communicating, creating and socialising) thus challenging the traditional concept of learning in a school setting.

It is important to note that

- While the digital world presents unlimited opportunities there are also some risks that need to be considered. Participating in social media is subject to the same standards of behaviour as those that apply when working with young people in the formal school setting.
- Staff who are interested in using social media tools to engage children and young people must have a clear educational context to support the teaching and learning.
- Staff have a duty to take reasonable steps to protect students from any harm that should have reasonably been foreseen and against which preventive measures could be taken.

## Social Media

Social media is the term used for internet based tools for sharing and discussing information among people. Additional social media tools may include (although are not limited to):

- Social networking sites (e.g. Facebook, LinkedIn, Instagram, Snapchat)
- Video and photo sharing websites (e.g. Flickr, Youtube)
- Blogs, including corporate blogs and personal blogs, micro-blogs (e.g. Twitter)
- Forums, discussion boards and groups (e.g. Google groups, Whirlpool) Wikis (e.g. Wikipedia)
- Vod and podcasts
- Video conferences and web conferences
- Email and instant messaging
- All other emerging electronic/digital communication applications.

## Examples of Acceptable Use of Social Media for Staff

The following examples demonstrate social media tools being used appropriately with a clear educational context:

- A philosophy teacher sends a weekly thought provoking question to use as a stimulus for a class discussion (Via Twitter)
- A principal reminds students of upcoming events at school such as 'at this week's assembly we will announce the school captains and SRC nominees.' (Via Twitter)
- An English teacher establishes a collaborative forum (set up for professional use only) to discuss issues or share ideas (Via Edmodo)
- A teacher asks her students to brainstorm their expectations for using a blog, including rules for online behaviour, giving feedback and the key elements of the post e.g. spelling, punctuation, accuracy of information, etc (Via Padlet or Global2.vic.edu.au)
- A principal establishes a 'group' for teachers to share professional learning opportunities, current research documents, meeting times and dates and reminders (Via Google drive)
- A humanities teacher tweets snippets of current events (relevant to the humanities curriculum) and shares links to key websites for more information. (Via Edmodo or Twitter)
- A class is assigned the task of designing and creating an interactive digital poster that demonstrates the students' knowledge, ideas and opinions of a particular subject under study (Via Canva).

## Examples of Unacceptable Use of Social Media for Staff

- Defining an official Dandenong High School social media account without the express written permission of the Principal
- Instigating or participating in 'chats' of a personal nature with students or parents via instant messaging
- Contacting parents regarding any matter via social media tools. All official communication to parents should be done by House Leadership Teams, using phone or email only.
- Instigating or participating in offensive or slanderous 'chats' regarding the school, a colleague (past or present), student (past or present) or parent (past or present) via DET instant messaging systems
- Contacting a student via written or electronic means including email, text messages without a valid educational context
- Using your DET email address for casual and personal emails that may be deemed as pornographic or offensive
- Adding or accepting a student to a personal social networking site as a 'friend'
- Downloading copyright protected content (images, music, etc) using any DET ICT system
- Using a DET email address to subscribe to web-based applications that are not for educational purposes

- School staff do not deliberately access sites that do not have a valid educational purpose when using school owned devices which can now include staff laptops, smart phones, netbooks, desktops, iPads, tablets etc.
- School staff who accidentally access inappropriate sites that are not educational when using school owned devices should notify their IT Manager and leadership team to establish whether further action is required to block access to the content or erase the history.

## School staff must not:

- share content from their personal social media site with students.
- post images of themselves on social media sites that have the potential to negatively affect their reputation.
- express personal opinions or make judgements regarding work or post-work related issues (regarding the workplace or colleagues) on a social media site or blog.
- email a personal opinion regarding DET policies to a newspaper website via a DET email system (e.g. Edumail).
- reveal personal and/or political opinions/bias on a social networking site using a network and/or computer owned or leased by the DET (Staff laptops are school owned)
- establish a social networking site for discussion of sensitive issues.
- post photos or messages of a sexual or offensive nature in an open forum.
- store any images in online storage spaces without applying the necessary privacy settings.
- allow students who are under the defined age to register for a social media tool where the terms and conditions require them to be that defined age.
- misrepresent themselves on a social media site.

## Expectations regarding social media use for Dandenong High School staff:

As a professional working at DHS, all staff are expected to act in a manner that reflects their standing in the community; that of a respectful and responsible citizen. It is imperative that staff always reflect on how they conduct themselves online.

**Staff need to ask themselves whether what they are about to post could cause offence to anyone or be thought inappropriate or bring the school into disrepute, because teachers are held to higher standards than most members of the public. If the answer is yes, or staff are not sure, then staff do <u>not</u> make the post.**

As part of staff responsibilities in meeting school expectations regarding the use of social media, all staff need to ensure the points on the next page are closely adhered to.

- Before uploading photos, visual images or videos of students on an online space, specific written permission should be sought from the student or their parents / guardians using the relevant permission form as found on the DET website. **The School's standard release form is not adequate for this purpose, as it only covers normal school operations or publications.**
- Staff should seek the consent of parents/guardians for students to participate and register to use social media tools.
- Staff will be required to gain parent / guardian consent to upload information, images and videos of the students. This is very important as a failure to obtain this consent may amount to a breach of privacy.
- If staff decide to use a social media tool for classroom/professional use then it is recommended that staff create a completely separate online space for this purpose. This online space should be treated with the same professionalism as is displayed at school. All correspondence and content that is uploaded must have a clear educational context/purpose.
- Consider whether staff need specific permission to upload content. Content may have copyright protection or may require specific permission before it can be uploaded.
- Privacy options and settings are extremely useful to protect online identity and professional reputation but they are not fool proof. These settings can be changed by the owners of the tool who do not always have an obligation to inform their users. The best way to maintain your professional image is to manage your profile professionally and regularly check for updates to Terms and Conditions that may occur. When using social media tools it is prudent to err on the side of caution.
- Expected behaviours for IT use are outlined and communicated to students and their families within the school's *Acceptable Use Agreement*. These include appropriate language and behaviours and the consequences for behaving inappropriately. It is essential that these same rules are understood for the online classroom/professional space.
- Staff should consider the content they upload or view and whether it reflects the professional image of staff and how you wish to be perceived by others.
- Staff should consider whether the content is detrimental to the standing of staff and the school in the community.
- Staff should consider whether friends or others can upload content to that staff member's social media site that may adversely affect the reputation of staff or the school
- Staff should consider whether their personal information could potentially be copied from their social media site and shared with a wider audience.
- When setting up or subscribing to groups, staff should keep in mind their professional status and how these groups may or may not uphold your professional image.
- It is important to note the history of reading and viewing activity may be highlighted and shared on personal profiles staff have set up on social media. Staff should consider how your professional image could be protected by using the privacy and filtering options that are available within the particular social media tool being utilised by staff.
- Staff are able to use cloud-based storage such as Google Drive and Dropbox as part of completing school-related tasks. However, staff should be aware that if they receive inappropriate materials via cloud-based storage services, then they should follow the procedures under "A Step-by-Step Guide for Removing Inappropriate Content from a Website, Facebook or other Social Media Site" attached to this policy, and inform the Executive Leadership Team of the incident without delay.

## Misuse and Legal Consequences

If you use the school's computer systems, school owned laptops or other electronic devices for personal use the school reserves the right to monitor such use including use of the internet and personal use of social media.

Unauthorised or inappropriate use during working hours will result in disciplinary action.

Misuse of social media may involve:

(i) a breach of employment obligations

(ii) serious misconduct

(iii) sexual harassment

(iv) unlawful discrimination

(v) a criminal offence, including

a. Menacing, harassing or causing offence

b. Child pornography

c. Stalking

d. Defamation

e. Copyright

(vi) a threat to the security of Department ICT resources

(vii) an infringement of the privacy of staff and other persons such as students or parents, or

(viii) exposure to legal liability.

**Evaluation: This Policy will be reviewed as part of the school's three year review cycle.**

**School Council Endorsement date: 21st June 2022**

Department of Education and Early Childhood Development

# A Step-by-Step Guide for Responding to Online Incidents of Inappropriate Behaviour Affecting Students

**School Staff Duty of Care**
Schools have a duty of care to take reasonable steps to protect students from any harm that should have reasonably been foreseen. The nature and scope of the duty in these circumstances will vary according to a number of factors, for example: the role and responsibilities of the employee, whether the incident occurred inside or outside of school hours, etc.
You are concerned about a student because you have:

- received a disclosure from the student who has been subjected to inappropriate behaviour that is occurring or has occurred in the digital world.
- received a report from an adult or another student about inappropriate behaviour that is occurring or has occurred in the digital world.

For further information visit about Duty of Care: www.education.vic.gov.au/management/lol/manage/care.htm

## Step 1 IDENTIFYING CONCERNS

**An incident of concern may include one or more of the following:**

**An event which causes distress to a student** including cyberbullying, sexting, exposure to pornographic images or a breach of the school's Student Engagement Policy.

**A student has been EXPOSED to and affected by inappropriate behaviour online and:**

The student is at risk of suffering significant physical, psychological or emotional harm and may be in need of immediate protection.

**Go to Step 3**

**A student has ENGAGED in inappropriate behaviour online that:**

a) May cause psychological or emotion harm to another student(s).
**Go to Step 2**

b) Could be deemed as criminal activity.
**Go to Step 3C**

c) Could be psychologically and/or emotionally damaging to themselves (e.g. sexting).
**Go to Step 2**

## Step 2 FURTHER ACTIONS

If you suspect that inappropriate behaviour has occurred, it is important to make sure the student/s are in a safe environment. It is also important to take detailed notes of the action that may include one or more of the following:

**A.** Inquire into the inappropriate behaviour. This may include discussions with all staff/students who have been directly or indirectly in the incident and/or its effects.

**B.** If you become aware during your inquiry that a criminal offence may have occurred contact the relevant authorities.
**Go to Step 3B & C**

**C.** Where appropriate, contact the parents of all students involved.
*If a school is unsure whether parents should be contacted, the Department's Legal or Emergency and Security Management Unit can assist to make a decision.
**Go to Step 3D**

**D.** Provide reasonable and ongoing wellbeing support to all students and staff who were involved in or witness to the incident.
**Go to Step 4**

**E.** Where appropriate, refer to the school's Student Engagement Policy and follow the appropriate processes and procedures.
**Go to Step 5**

## Step 3 REPORTING

**A. Report to School Leadership**
Staff member immediately advises and consults a member of the school's leadership team to report the incident and plan the appropriate response.

**B. Report to Emergency and Security Management**
All reportable incidents should be reported to Emergency and Security Management Unit (03 9589 6266). This will alert regional staff.

**C. Report to Victoria Police**
It is expected that an staff member will contact police if there has been possible criminal activity. In such cases seek advice about contacting the parents of ALL students involved in the incident.
*If a school is unsure whether an incident should be reported the Police will advise the school as to whether they will investigate or whether the school should handle the situation.

**D. Report to Parents and/or Guardians**
Contact the parents/guardians of the student who has been exposed to and/or engaged in inappropriate behaviour (where appropriate).
*If a school is unsure whether parents should be contacted, the Department's Legal or Emergency and Security Management Unit can assist to make a decision.

**E. Provide a Wellbeing Referral and Support**
Consult with relevant regional staff as appropriate.
**Go to Step 4**

## Step 4 WELLBEING REFERRAL

**Wellbeing Referral**
Contact your school's Leadership and/or Student Wellbeing Team to discuss strategies that can be used to respond to and support ALL students at risk from the inappropriate behaviour. This may include counselling and support or the development of an action plan to implement targeted strategies.

Keep a record of the action plan and make notes on any relevant observations. Review the action plan as necessary.

## Step 5 ACTIONS AND CONSEQUENCES

Each Victorian government school has developed a Student Engagement Policy that sets out the rights, responsibilities and shared expectations of everyone in the school community, including students, parents, teachers and school staff. The policy clearly defines the consequences for students who behave inappropriately. In responding to online incidents of inappropriate behaviour, principals and teachers should refer to their Student Engagement Policy for appropriate actions and consequences.

For additional information, see:
Building Respectful and Safe Schools Resource
www.education.vic.gov.au/respect

Department of Education and Early Childhood Development

# A Step-by-Step Guide for Removing Inappropriate Content from a Website, Facebook or other Social Media Site

**Inappropriate content may include but is not limited to:**

- Words or images that personally attack, humiliate or defame an individual.
- Content that threatens, discriminates, harasses, menaces or causes offence including stalking.
- A fake profile of an individual or school.
- Content that is illegal, gives instructions for illegal activity or advocates terrorist activities.
- Depictions of nudity, pornography or child abuse.
- Depictions of excessive violence.

**At all times remember to:**

- Record the incident.
- Record the process taken to resolve the incident (e.g. steps taken to remove content, mediation attempts).

## Step 1 REMOVING CONTENT

If you know the person responsible for the content then ask the appropriate person for it to be removed.

If the person is unknown, cannot be contacted or refuses to remove the content.

**Go to Step 1a**

### Step 1a

Most websites (see reverse) where users can post their own content have established processes for removing inappropriate content. They often rely on users reporting content to the site administrator so they can act.

It is advisable to check the terms and conditions of any website you wish to remove content from for information to help you.

The procedures for some popular social media websites are available on the back of this document. If you need assistance your school technician may be able to help.

If the website administrators will not remove the content as per your request and you believe it should be removed.

**Go to Step 2**

## Step 2 CENTRAL OFFICE SUPPORT

**ITD Risk Management**
Provision of support for incidents that relate to the defacement of a DEECD website.
Ph: 03 9637 3586

**Legal Services**
Provision of advice to regions and school principals on legal issues arising from the content uploaded to social media sites.
Ph: 03 9637 3146

**Emergency and Security Management Unit**
A 24 hour/7 day a week single reference point to report *emergency* matters and *critical* incidents including criminal and unwanted activities.
Ph: 03 9589 6266

**Go to Step 3**

## Step 3 GOVERNMENT AGENCY SUPPORT

If you believe that the content may be illegal or prohibited*, you can report it to the following authorities:

**Australian Communications and Media Authority**
If you have found something offensive online and/or potentially prohibited content online and the website will not remove it you can report it via the ACMA hotline at www.acma.gov.au/WEB/STANDARD/pc=PC_410099

**Victoria Police**
If you believe that the posting of the content constitutes criminal activity it should also be reported to Victoria Police.

* *Under the Broadcasting Services Act 1992, prohibited content includes but is not limited to: child abuse images, unrestricted access to pornography, excessive violence, illegal activities, and terrorist-related material.*

Department of Education and Early Childhood Development

# A Step-by-Step Guide for DEECD Employees to Access Legal and Wellbeing Support for Online Incidents of Concern

**Legal and Wellbeing Support**
A DEECD employee within a school setting may require legal or wellbeing support and advice from the Department's Regional and/or Central office if:

- they have been the personal subject of online vilification (personally attacked, humiliated or defamed) by a student, parent/community member
- the school has been the subject of online vilification (unreasonable criticism, fake website or social media profile) by a student, parent/community member

**At all times remember to:**

- Record the incident (e.g. take a screen shot of the offensive material)
- Report the incident to the appropriate management (e.g. principal, Regional Network Leader) and inform colleagues when appropriate.
- Record the process taken to resolve the incident (e.g. steps taken to remove content, mediation attempts)

## Step 1 SCHOOL BASED ACTION

An incident whereby a DEECD employee has been vilified online by a student, parent, etc causes significant distress to the teacher and they require wellbeing and/or legal support and advice.

**1.** If the concern relates to a teacher or staff member other than yourself and you have formed the belief that they are at risk of harm and in need of immediate support.
**Go to Step 4, then 5**

**2.** If the concern relates to a teacher or staff member and they are not at risk but require support that is outside the school's capacity.
**Go to Step 2**

**3.** If the concern relates to a teacher or staff member other than yourself and you have formed the belief that they require a referral to support their wellbeing.
**Go to Step 5**

*You are NOT the principal*
**4.** In the first instance, speak to your principal about the support that is available at your school.

*You are the principal*
**5.** If you require support in managing an online incident of concern.
**Go to Step 3**

**6.** If you require advice and support in taking disciplinary action against a student, see the *Step-by-step Guide to Responding to Online Incidents of Inappropriate Behaviour by Students.*

## Step 2 REGIONAL OFFICE SUPPORT

Regions can work with principals and teachers to manage an issue. They can provide support with the interventions necessary to resolve an issue and refer the employee to the appropriate central office support and/or external agency support.

For support with a concern or issue contact your Community Regional Liaison Officer.

| | |
|---|---|
| WMR: | (03) 9291 6500 |
| EMR: | (03) 9265 2400 |
| SMR: | (03) 9794 3555 |
| LMR: | (03) 5440 3158 |
| GR: | (03) 5337 8480 |
| BSW: | (03) 5225 1000 |
| GIPP: | (03) 5127 0400 |
| HUME: | (03) 5761 2100 |
| NWR: | (03) 9488 9488 |

## Step 3 LEGAL SUPPORT

**Conduct and Ethics Unit**
Provide advice to school principals in relation to managing complaints involving the conduct of DEECD employees. Phone: (03) 9637 2594

**Legal Services Unit**
Provide advice to regions and school principals on legal issues relating to social media. Phone: (03) 9637 3146

If a DEECD employee requires additional wellbeing support outside of the school's capacity.
**Go to Step 5**

## Step 4 REPORTING

**Emergency Services**
If you believe a criminal offence has occurred then you should consider making a report to Victoria Police.

**Emergency and Security Management Unit (ESM)**
This is the DEECD's 24 hour/7 day a week reference point to report emergency matters and critical incidents.
Phone: (03) 9589-6266.

**Edusafe**
This is the DEECD's Incident Reporting & Hazard Management System. Users can report an incident or hazard they have sustained or witnessed. To make a report log into www.eduweb.vic.gov.au/edusafe

For additional wellbeing advice and support.
**Go to Step 5**

## Step 5 WELLBEING SUPPORT

**Employee Assistance Program**
A free service that offers self-referred, short-term, confidential counseling for personal and work concerns.

**Manager Assist**
A telephone advisory service providing management advice and support to principals and workplace managers.
Phone: 1800 337 068

**Employee Health Unit**
Provide further information regarding these and other support services available to DEECD employees.
Phone. 03 9637 2460.

*Adapted from http://www.education.vic.gov.au/school/principals/spag/governance/pages/socialmedia.aspx*