NTSDE 40th Anniversary
'Education Wherever You Are'
NT School of Distance Education

(08) 8922 2222

ntsde.admin@ntschools.net

PO Box 40471, Casuarina NT 0811

The Bullocky Point Education Precinct
Atkins Drive, The Gardens, NT 0820

Teaching and Learning Online Cyber Security Considerations

Establishing Protocols

Working online with students requires establishing protocols to enable a safe and inclusive environment.

Explicitly teach protocols for using any online platforms e.g.

- use appropriate language when creating nick names, using chat functions and interacting with others online
- ensuring that only appropriate content is shared during screen sharing
- maintaining confidentiality other people when working from home such as not having pictures of friends in the background or family members walking through during the lesson
- do not type over or delete other students' work in shared documents.

Explicitly teach students how to appropriately participate in online synchronous lessons (video conferencing)

- do not share meeting room details with other people
- welcome each student individually/have all cameras on at the start of lessons to ensure only invited participants are in the 'virtual room' (also a good opportunity to record attendance)
- be aware of your surroundings and use headphones if possible. If around others, keep the microphone on mute unless speaking. This helps to ensure sensitive conversations aren't accidently overheard and also minimizes feedback
- use the Raise Hand function and wait to be asked to speak or add questions to the chat box
- allow time for any internet 'lag' when someone is speaking
- only having school related apps and content open when screen sharing with the rest of the class or during Breakout Rooms.

Maintaining Confidentiality

Using online tools can potentially expose students to data mining and safety issues. The Department of Education Intranet has a number of online and cloud apps which have been reviewed and approved http://ed.ntschools.net/digdata/Pages/Systems.aspx. Other applications that require student accounts can put students potentially at risk and DoE approval needs to be sought to use them for classroom purposes. Teachers need to also be aware of the potential negative impact on student learning when they have to learn how to navigate and use multiple platforms and applications particularly when different teachers are using different options.

There are also online apps that are available that do not require students to create accounts or use personal information which can be used for example Kahoot https://kahoot.it/ and Nearpod https://nearpod.com/ where students join online using a code provided by the teacher.

The eSafety Commissioner website https://www.esafety.gov.au/ has many useful resources for maintaining cyber safety including:

- Classroom resources https://www.esafety.gov.au/educators/classroom-resources
- Cyberbullying https://www.esafety.gov.au/key-issues/cyberbullying
- Toolkit for schools https://www.esafety.gov.au/educators/toolkit-schools

When using web conferencing tools there are some ways that you can increase security such as limiting how the meeting room details are shared and using passwords.

See https://www.cyber.gov.au/publications/web-conferencing-security for more information.

Protective Practices for Teachers

The TRB outlines protective practice guidelines https://www.trb.nt.gov.au/protective-practice-guidelines (page 9) outline appropriate practices for working with students in an online environment. When working with students individually it is important consider if parents/guardians are aware and the interaction is conducted in a public space in the home. If not practical the recording feature in Zoom could be used when working with individual students as a protective measure.