Defence Youth Safety Fact Sheet
Cyber Safety for Parents

Cyber safety is everyone's responsibly but as a parent of a child involved in a Defence Youth Program there are some very simple steps you can take to keep you and your children safe.

Tips for securing devices

To ensure that devices are secured:

- Install parental control software to block and restrict access to unwanted content.
- Ensure all software is up to date and correctly configured.
- Use a reputable anti-virus product and set it to regularly update and automatically scan.
- Backup data regularly to a different device to prevent data loss.
- Be wary of unsolicited phone calls and emails.
- Check and configure security and privacy settings on all sites and devices.
- Use strong passwords and make sure that every account has a different password.
- Always use legitimate software from a reputable source.
- Enable remote tracking and remote wiping functionality, if supported by your device, in case the device is lost.

Communicating and encouraging safe behaviour

Encouraging your child to think before they post anything online and educating them about safe, responsible and positive online behaviour is important in helping them stay safe online. To achieve this, you can:

- Set rules on the use of devices and the internet, being sure to seek input from your child.
- Explain the dangers of meeting face to face with someone they have met online and that people they chat to online may not be who they say they are.
- Encourage your child to talk about their online activities especially if they see something they are uncomfortable with.
- Talk to your child about cyber bullying and ensure they know how to block and report people if they are having issues.
- Help to keep your child's information safe by ensuring they use strong passwords, correctly configure privacy settings and avoid using personal information where practical.

If you or your child utilise Australian Defence Force Cadets (ADF Cadets) provided ICT systems, it is important to know that these systems are governed by acceptable usage policies and it is the user's responsibility to ensure that they do not breach these policies. Users of these systems are individually responsible for maintaining the security and integrity of their ICT account(s), and it is the responsibility of the owner to ensure devices used to access ADF Cadets provided ICT systems are appropriately secured. The Cyber Safety for Young People Fact Sheet can be accessed at www.defenceyouth.gov.au

Further Information

More detailed information can be found online at StaySmart Online, eSafety.gov, and the Office of the Australian Information Commissioner and you can report cybercrime at ACORN or cyber bullying at eSafety.gov.