Cybersafety and Digital Technology Policy

INSTRUCTIONS FOR PARENTS AND CARERS

a. Please carefully read through this policy.

b. Discuss this policy and the *'Responsible Use Agreement'* with your child.

c. Sign the *'Responsible Use Agreement'* page of this policy and return it to Reception or complete the Acceptance page via Operoo.

d. Keep a copy of this policy as a reference.

PURPOSE

The purpose of this policy is to outline the measures Belgrave Heights Christian School uses and the expectations the School has to ensure the safety of students in relation to the use of Digital Technology and the internet.

DEFINITIONS

BYOD – Bring Your Own Device. This was the original name of the program which facilitates students bringing Digital Devices/Digital Technology to School for educational purposes. This is now known as the Digital Device Program.

Cyberbullying – is carried out through the use of Digital Technology. This includes, but is not limited to social media, chat programs and email. Harassment and bullying both involve behaviour that intends to harm its recipient through threats, intimidation, victimisation or humiliation. Harassment is any conduct that negatively targets a person based on their race, sex, religion, gender or disability.

Cybersafety – also known as internet safety or eSafety, is an individual's awareness of online dangers, and putting measures in place for the safe use of the internet and internet connected devices.

Digital Technology – incorporates the School's computer network, internet access facilities, computers and other technology equipment/devices including, but not limited to desktop computers, laptops, tablets, storage devices such as USB and flash memory devices, CDs, DVDs, webcams and mobile phones, printers and photocopiers. This includes both School owned and personal devices.

Digital Device – incorporates desktop computers, laptops, tablets, smart watches and mobile phones.

Minimum Specifications – relates to student owned personal devices as per the Minimum Specification Sheet. This will be dependent on the year level of the student. (Does not apply to Year 7 and 8)

Objectionable – in this agreement means material that deals with matters such as sex, cruelty, or violence, in such a manner that it is likely to be detrimental to the wellbeing of students or other individuals, and is not considered to be in line with the School's values, or is incompatible with a school environment. This is in line with the definition used in the *Classification (Publications, Films and Computer Games) Act 1995*.

Responsible Use Agreement – the Agreement that upon signing becomes the acknowledgement to agree to abide by this policy.

The School – Belgrave Heights Christian School

DIGITAL DEVICE PROGRAM INFORMATION

The School's Digital Device Program aims to provide the opportunity for each student to use Digital Technology during the course of their education. This includes both school-owned and student owned devices.

YEAR 7 AND 8

There are a number of requirements for participation, this includes students participating in an induction program before Chromebooks are issued. Once all requirements have been met and the student induction has been completed, students will be permitted to take home their Chromebooks.

PREP – YEAR 12 (INCLUDING YEAR 7-8)

As part of the Digital Device Program, the Agreement must be signed by students and parents/carers in relation to the use of Digital Technology at School. This Agreement supersedes all previously signed agreements relating to Digital Technology use at School.

The School's Digital Technology is for educational purposes appropriate to the School environment. This applies whether the Digital Technology is owned or leased either partially or wholly by the School, and used on or off the School site OR where a BYO device is used at School for, or during, School activities.

The School monitors traffic and material sent and received while someone is using the School's computer network and uses filtering and monitoring software to restrict access to certain sites and data, including email. The School audits its computer network and related Digital Technology and may commission an independent forensic audit of Digital Technology.

MINIMUM SPECIFICATIONS (Student Owned Devices YEAR 9 - 12)

Device Type	Windows Laptop	Mac Laptop	Windows Surface	Chromebook
Operating System	Windows 10	OSX 10.7	Windows 10	Chrome OS
Wireless	5GHz 802.11a/b/g/n	5GHz 802.11a/b/g/n	5GHz 802.11a/b/g/n	5GHz 802.11a/b/g/n
Screen Size	11"	11"	10"	11"
Storage	64 GB hard drive	64 GB hard drive	64 GB hard drive	32 GB hard drive
RAM	4 GB	4 GB	4 GB	4 GB
Battery Life	6 hours	6 hours	6 hours	6 hours
Examples*	**1**	**2**	**3**	**4**
Warranty	An extended warranty and accidental damage insurance plan is suggested but not mandatory.			

** Current as at September 2022*

Examples

1. **Windows Laptop:** https://www.orderportal.com.au/CompareDevices?ofid=131&pids=3995320
2. **Mac Laptop:** https://www.apple.com/au-hed/shop/buy-mac/macbook-air
3. **Windows Surface:** https://www.orderportal.com.au/CompareDevices?ofid=131&pids=4019139
4. **Chromebook:** https://www.orderportal.com.au/CompareDevices?ofid=131&pids=3820916

SPECIAL NOTE FOR MINIMUM SPECIFICATIONS FOR ART SUBJECTS

Currently it is essential that students intending to undertake Art and Design subjects in Years 9, 10, 11 and/or 12 have a suitable laptop that is able to run Adobe Creative Suite (e.g. Adobe Photoshop) programs. Some laptops, like a Chromebook, are not able to run Adobe Creative Suite, and may limit the Art and Design subjects available to students. The subjects that this applies to includes, but is not limited to: 9/10 Photography and Digital Design, 9/10 Visual Communication, 11/12 Studio Arts, 11/12 Visual Communication Design. The School continues to review this as technology changes.

ACCEPTABLE USE

The School has provided guidelines in this document in relation to the acceptable use of Digital Technology and the School's internet.

All students and their parents/carers are required to sign the **Responsible Use Agreement** connected to this policy, which covers the care, use and management of Digital Technology in a cybersafe learning environment. This management covers security, email, internet access, virus protection and cybersafety.

The use of Digital Technology is for the benefit of students' learning. The permissible use of Digital Technology is on the understanding that students will access applications and files in safe and ethical ways. Students need to be aware that the **School's Student Code of Conduct** (accessible from the School's website) extends outside of school hours and off site.

In the case of online learning, both on and off school premises, students and parents/carers should also be aware of the **School's Online Learning Policy** (accessible from the website).

The School reserves the right to monitor the content of any Digital Technology used on the School's network for the purpose of acceptable use. This includes email and network filtering, as well as Digital Technology monitoring. This is done as part of the School's child safety principles and security measures.

CYBERSAFETY & CYBERBULLYING

Belgrave Heights Christian School is committed to creating a cybersafe learning environment. We work in partnership with families towards reducing the risks of abuse and harm that can occur in a virtual environment. Please refer to **Cybersafety Guidelines** provided in this document to help everyone stay safe when using Digital Technology at School and outside of normal school hours. Please refer to the **Online Learning Policy** for specific guidelines regarding Online Learning.

As per the **Student Code of Conduct** (available on our website) and the **Bullying & Harassment Policy** (available on our website), students must not participate in any form of cyberbullying, or behave online in a manner that threatens, intimidates, victimises or humiliates another child, student, parent or member of the School Community. This includes, but is not limited to the sending, posting or distributing of inappropriate and hurtful email messages, instant messages, text messages, digital pictures/images, social media and/or website postings.

Whether this behaviour occurs off site, on site, during school hours and/or out of school hours, the School reserves the right to suspend or exclude a student from attendance at school should there be a breach of any of these policies.

If the School suspects a cybercrime has been committed, the School has an obligation to report this to Victoria Police under the Cybercrime Act 2001 and the Criminal Code Act 1995. Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on Digital Technology e.g. mobile, laptop or USB/storage device, the relevant item of Digital Technology will be confiscated and handed to the investigating authority. The Police will determine any further action that may need to be taken.

Where the School is contacted by the Police in relation to a crime that involves the use of digital technology the School is legally obligated to provide the contact details for the parties involved in the crime.

USING THE SCHOOL'S NETWORK AND BREACHES OF THIS POLICY

Students must only connect to the School's network and/or internet for the purposes of education while on premises at School. The following actions are considered to be unacceptable by the School and in breach of this policy:

a. Using a mobile hotspot (e.g. mobile phone data sharing, or another similar device).
b. Connecting to the Internet through a proxy or VPN service.
c. The use of chat clients (e.g. Messenger), or playing LAN games.
d. Downloading large, non-school related files.
e. Changing of any network settings.
f. Attempting to remove any internet filtering software installed by the School.

Accessing Sensitive, Offensive and Objectionable Material

Students must not make any attempts to try to find information that could harm, embarrass or offend. If students should accidentally come across sensitive, offensive or objectionable material they must minimise or turn off that screen immediately and report this to a teacher or other staff member. The retrieval, viewing, sharing or posting of any objectionable material that is sexually explicit, obscene, violent, or offensive is prohibited.

Divulging personal information

Students must not divulge any personal information about themselves or others (e.g. home addresses, telephone numbers, EFTPOS or credit card numbers, date of birth, age) online unless expressly requested to do so by a teacher or staff member for educational purposes.

Invading privacy and sending anonymous messages

Students must not attempt to invade the privacy of others, send anonymous messages or, messages with offensive language. Students are reminded that their School email accounts are not private and that filtering is in place. This filtering may flag offensive language or objectionable material.

Monitoring of software

The School reserves the right to install educational and/or monitoring software on BYO Digital Devices used at School as deemed necessary, for both the safety and enhancement of student learning. Families must not attempt to remove any software installed by the School without first consulting with the IT Department.

NON-SCHOOL APPLICATIONS, COPYRIGHT, MUSIC & MEDIA FILES

Removal of problem software

At all times, the performance of Digital Devices is for the primary purpose of student learning. Some software can slow down the performance of the Digital Device or corrupt it so that it is unusable. The School may not support software installed by students. If software is installed by a student that creates an issue on a student's Digital Device, the IT Department will remove the problem software.

Copyright Law and Intellectual Property Rights

Students must adhere to any laws pertaining to copyright (*Copyright Act 1968 (Cth)*), other intellectual property rights and licensing agreements. All software, music, games, images, and material on a student's Digital Device or Digital Technology must not be in violation of any laws. The downloading, sharing, storing, and playing of illegal or pirated material is prohibited. Any illegal material discovered during the course of a Digital Device or Technology audit, repair or upgrade will result in the illegal material being deleted immediately. Students are permitted to store legally downloaded music and other media on their Digital Devices.

Digital Devices with Illegal Content

Digital Devices or Digital Technology that fall under the School's Digital Device Program found to contain illegal content may be re-imaged or restored to factory settings dependent on the nature of the material discovered during an audit. This is also dependent on the type of device, in the case of mobile phones, the device may instead be confiscated. In some instances, dependent on the nature of material found, the device may be provided to the police. It is therefore important to ensure that students have backups of the information stored on their Digital Devices in an alternative location as good practice. Equally, a breach of the School's policies on the use of non-school applications may also result in the restoration of the Digital Device to its original specifications, with the consequential loss of all student data.

CARE AND SECURITY OF DIGITAL DEVICES

The onus is on students to take care of their Digital Devices and Digital Technology in relation to carrying, cleaning, storage and security both on and off-site and to treat their Digital Device with the appropriate level of care. This applies to both School owned and personal Digital Devices. Students experiencing problems with their device are generally referred to the IT Department who are able to provide basic support.

Damage to Digital Technology

Damage to Digital Technology belonging to the School due to neglect, abuse or a malicious act, will have the cost of repair or replacement passed on to the parent/carer for payment, as per the School's **Fees Policy** and **Enrolment Terms and Conditions** (available from the School's website).

Year 7-12: Students are expected to bring Digital Devices fully charged to school each day. For Occupation Health and Safety reasons, chargers should not be taken to school.

Lost, Stolen or Damaged Digital Devices

Parents/Carers must ensure that students report lost, stolen or damaged Digital Devices to the school within 24 hours of the incident occurring. If a Digital Device has been lost or stolen, it must be reported to the police. The School does not accept any liability for lost or stolen Digital Devices, as per the Enrolment Terms and Conditions and the Parent Handbook (copies are available on the School's website). For this reason, it is important that all students have the appropriate locks for their School locker.

REPAIR AND MAINTENANCE OF CHROMEBOOKS (YEAR 7, 8 AND APPLICABLE YEAR 9, 2022 ONLY)

The Chromebook is covered by a three-year manufacturer's warranty, excluding damage due to accidents, liquid spills, submersion and unauthorised service or modification. The School will provide basic hardware, software and network support. Students are asked to see the IT Department if they are experiencing issues with their Chromebook during the course of a school day.

For families who choose to take up this option, Accidental damage is covered by insurance. This does, however, involve an excess being charged. At the time of printing, this excess charge is $150. The family of a student who is found to have wilfully damaged or caused repeated careless damage to their Chromebook will be liable for the full repair cost of the Chromebook.

The School has an expectation that repairs to Chromebooks are attended to in a timely manner. The device should ideally be repaired within a 30-day time frame. In cases where this is not possible and proof can be provided, the School has a limited supply of loan devices, which can be used, dependent upon availability.

'LOAN' DIGITAL DEVICES

Belgrave Heights Christian School has available a limited supply of 'loan' Digital Devices for students to use if their Digital Device is unavailable due to repair or if they are in a year level where they are not yet required to own their own Digital Device. These Digital Devices are generally not available to students who have simply forgotten their Digital Device at home. 'Loan' Digital Devices are not available for students to take home, except in the case of mandated 'remote' learning (e.g. school closure). The same care and Acceptable Use applies to 'Loan' Digital Devices.

RESPONSE TO BREACHES OF THIS POLICY

Adherence to this policy, and its guidelines, will help ensure a positive, supportive, productive, and safe learning environment for all students at Belgrave Heights Christian School. Students must adhere to the directions of teachers and staff at all times. Students should not attempt to open any application or file unless instructed to do so by a teacher. Depending on the seriousness of a particular breach of this Agreement or other policy, an appropriate response will be made by the School. Possible responses could include one or more of the following:

a. a discussion with the student
b. informing parents or carers of the incident
c. loss or suspension of student access to the School's Digital Technology network, resources or facilities
d. taking disciplinary action
e. recovery of any incurred costs
f. removal and confiscation of a Digital Device/Digital Technology from a student's possession
g. if illegal material or activities are involved, it may be necessary for the School to inform Victoria Police.

CHANGES TO THIS AGREEMENT

The School reserves the right to amend this Agreement as necessary. These changes may be brought about due to changes in technology, legislation, or policy. Any changes will be communicated in writing.

Cybersafety Guidelines

Parents and carers play a vital role in helping to develop knowledge, understanding and ethics around their child's safety, particularly when using a Digital Device and the internet. Parents and carers are also important partners in helping their children to employ cybersafe practices for themselves and the people around them. We encourage families to take time to discuss the strategies listed here to help children in staying safe when using Digital Technology both in and out of school. Some helpful guidelines for students to know and adhere to have been listed below.

1. I will not use the School's Digital Technology until my parents/carers and I have read, completed, signed and returned the Agreement Form to the School.
2. I will only ever log on with my own username. I will not allow anyone else to use my username or log-on. I will also not use somebody else's log-on, even if I know the details.
3. I will not impersonate or pretend to be anyone else online and will not alter my online profile to anything different to that created by the school.
4. I will keep my password private and will not share it with others.
5. I will only connect a Digital Device to the School's network with permission from the teacher. This is also true for any software brought to school on a Digital Device (e.g. a USB/portable drive, camera or phone). It also includes all wireless/Bluetooth technologies.
6. I will only use my Digital Device and the internet at School, when a supervising staff member gives me permission to so or for the purposes of homework/study and assignments.
7. I will only use the internet, email, Digital Devices (including mobile phones) or Digital Technology for positive purposes and not to offend, be mean, rude or to bully, harass, or harm anyone else in any way, or harm the School, even if it is meant as a joke.
8. My privately-owned Digital Technologies, such as a laptop, tablet, mobile phone, USB/portable drives that I bring to school are also covered by the Agreement. Any images or material on such devices must be appropriate to the School environment.
9. I will not use my mobile phone at School during the course of a school day unless I have the express permission of a staff member to do so.
10. I will not take screenshots or videos of other persons using Digital Technology without express consent and/or the required permission.
11. While at school, I will:
    a. Only access, attempt to access, download, save and distribute age appropriate material that is relevant to my education during the course of the school day.
    b. Report any attempt to get around or bypass security, monitoring and filtering that is in place at school.
12. If I accidentally access inappropriate material, I will:
    a. Not show others.
    b. Not forward it onto other users.
    c. Turn off the screen or minimise the window.
    d. Report the incident to a teacher or other staff member immediately.

13. I will inform the teacher of any involvement or activity involving Digital Technology that might put me or anyone else at risk while I'm at school and/or involved in School internet/Digital Technology activities (e.g. Inform on bullying or harassing).
14. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
    a. my full name
    b. my home address
    c. my email address
    d. my age or date of birth
    e. my phone numbers
    f. photos/videos of me and/or people close to me (particularly in school uniform).
15. I will not share anyone else's personal details or identifying information online.
16. I will ask my teacher's permission before I share Zoom links, school resources or school-related documents with individuals or organisations outside of the School community.
17. I will not use my BHCS email account to sign up for non-school related resources or platforms.
18. To ensure I comply with copyright laws, I will only download or copy files such as music, videos, games or programs when I have been given permission by a teacher or the owner of the original material. If I infringe the *Copyright Act 1968*, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs/applications.
19. The School may monitor traffic and material sent and received using the School's Digital Technology network. The School may use filtering and/or monitoring software to restrict access to certain sites and data, including email.
20. The School may monitor and audit its Digital Technology network and Internet access and may commission an independent forensic audit. Auditing may include any stored content, and all aspects of their use, including email.
21. I must not attempt to remove any software installed on personally owned or School owned devices without express permission from the IT Department.
22. I will respect all of the School's Digital Technology and will treat all Digital Technology care. This includes:
    a. Not intentionally disrupting the smooth running of any of the School's Digital Technology systems
    b. Not attempting to hack or gain unauthorised access to any system.
    c. Following all the School's cybersafety guidelines, and not joining in if other students choose to be irresponsible with Digital Technology.
    d. Reporting any breakages/damage or irresponsible use to a staff member.
23. If I do not follow cybersafe practices, the School may inform my parents/carers. In serious cases, the School may take disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or an e-crime is suspected, it may be necessary for the School to inform the Police and hold securely any personal items for potential examination by Police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

BHCS Student Digital Technology: Responsible Use Agreement

STUDENT AGREEMENT

I have read and understood the Cybersafety and Digital Technology Policy and understand my part in Responsible Use and being cybersafe. I have:

1. Read the Cybersafety Guidelines **OR** had it read/explained to me.
2. Read the Student Code of Conduct **OR** had it read/explained to me.
3. I am aware of the how the school's maintains the care, use and management of Digital Technology (including mobile phones) in a cybersafe learning environment.
4. I agree to abide by the policy and will not do things that cause me to put myself or others at risk by revealing information that I should not be revealing or by acting inappropriately.
5. I also agree to not try to get around the School's network in any way or delete any School-installed software and understand that this is there for my safety and the safety of others.
6. I understand that if my Digital Device/Digital Technology is found to contain Objectionable, illegal or suspect content that this will be deleted or this may cause my Digital Device to be restored to its original settings.
7. I understand that failing to abide by the Cybersafety and Digital Technology Policy and failing to follow the guidelines within this same policy and/or the Student Code of Conduct could result in disciplinary action being taken against me by the School.

DETAILS FOR STUDENT	
Child's First Name and Surname:	
Student Signature*:	**Date:**

*Prep – Year 2 students do not need to sign and should just have their name added to the form.

PARENT AGREEMENT

I have read and discussed the School's Cybersafety and Digital Technology Policy with my child and understand the role that I play in developing my child's knowledge with respect to cybersafety. I agree to partner with the School in relation to this and am aware of the School's initiatives to maintain the care, use and management of Digital Devices in a cybersafe learning environment. I further understand that breaches of the School's Cybersafety and Digital Technology Policy could result in:

1. A discussion with my child.
2. Being informed of the incident.
3. Loss or suspension of my child's access to the School Digital Technology network, resources or facilities.
4. Disciplinary action being taken.
5. Recovery of any incurred costs.
6. Removal/deletion of objectionable/illegal/suspect content from my child's Digital Device or the restoring of my child's device to its original settings.
7. Removal and confiscation of a Digital Device/Digital Technology from my child's possession.
8. If illegal material or activities are involved, it may be necessary for the School to inform Victoria Police.

DETAILS FOR PARENT/CARER	
Parent/Carer's First Name and Surname:	
Parent/Carer Signature:	**Date:**

Please return this page and keep a copy of the policy for your own reference

ADDITIONAL RESOURCES

The following websites contain valuable information for parents.

FOR RESOURCES ON CYBERSAFETY FOR PARENTS

Office of eSafety Commissioner	https://www.esafety.gov.au/parents
eSafety for Kids	https://www.esafety.gov.au/kids
Stay Smart Online	www.staysmartonline.gov.au
Thinkuknow	https://www.thinkuknow.org.au/
The Australian Institute of Family Studies	https://aifs.gov.au/cfca/publications/online-safety

The Australian Parenting Website

For pre-teens: https://raisingchildren.net.au/pre-teens/entertainment-technology
For teenagers: https://raisingchildren.net.au/teens/entertainment-technology

FOR RESOURCES RELATED TO AUSTRALIAN COMMUNICATIONS AND MEDIA

https://www.acma.gov.au

INFORMATION AND STRATEGIES ON HOW TO DEAL WITH BULLYING FOR PARENTS, STUDENTS AND SCHOOLS

http://www.bullyingnoway.gov.au/
https://kidshelpline.com.au/teens/issues/bullying

TO REPORT ONLINE BULLYING (CYBERBULLYING)

https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying

FOR INFORMATION AND SUPPORT FOR VICTIMS OF BULLYING

Kids Helpline	http://kidshelpline.com.au/
Lifeline	https://www.lifeline.org.au/
Reach Out	www.reachout.com.au
Beyondblue	www.beyondblue.org.au
Headspace	www.headspace.org.au
Australian Psychological Society	www.psychology.org.au
Australian Guidance and Counselling Association	www.agca.com.au

FOR INFORMATION ON CYBER CRIME

Australian Federal Police https://www.afp.gov.au/what-we-do/crime-types/cyber-crime

FOR COPIES OF THE CODES OF CONDUCT

https://www.bhcs.vic.edu.au/info/privacy-policy/code-of-conduct

Top 5 online safety tips for kids

1

Set up your device to protect your information.

2

Explore safely & tell an adult if you see anything online that makes you feel yuck.

3

Limit who can contact you when you're playing games.

4

Stop all contact with anyone online who asks you to do anything you don't want to do. Report and block them.

5

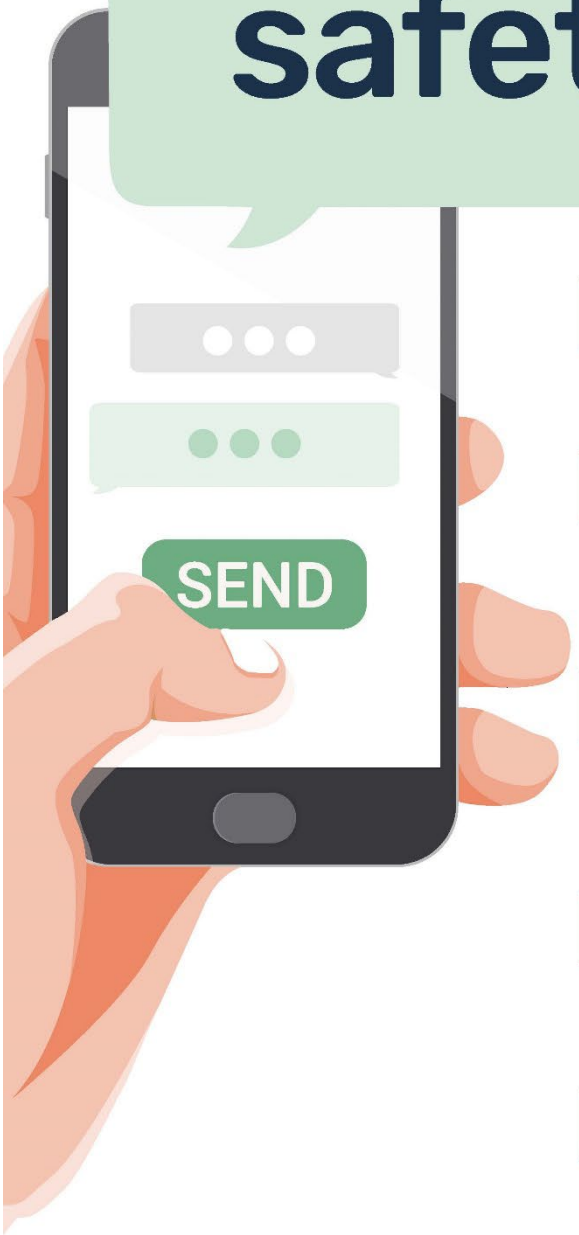
Ask for help if anything online is bothering you.

eSafetykids

esafety.gov.au/kids

Belgrave Heights Christian School

Top 5 online safety tips



1. **Think of others' feelings** before you post, like or share content.

2. **Ask for permission** before you share a photo or video with someone else in it. Respectful online relationships start with consent.

3. **Be an upstander** Speak up if you see someone cyberbullying or sharing nudes in a group chat – let them know that's not okay. Report and delete it.

4. **Use privacy and screen time** settings to take control of your digital life and its impact on your mental health.

5. **Ask for help** Cyberbullying and sharing intimate images without consent can be distressing, but eSafety can help remove them.

eSafetyyoungpeople

esafety.gov.au/young-people