Use of Digital Devices and Cybersafety Agreement

IMPORTANT NOTICE

Instructions for Parents and Guardians

1. Please read this agreement carefully.
2. Discuss the "*Use of Digital Devices and Cybersafety Agreement*" with your child.
3. Sign the "*Use of Digital Devices and Cybersafety Agreement*" attached and return this page to Reception.

The measures to ensure cybersafety at **Belgrave Heights Christian School** outlined in this document are based on the core values of the School.

The School's computer network, internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. This applies whether the ICT equipment 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 using the School's ICT network and uses filtering and monitoring software to restrict access to certain sites and data, including email. The School audits its computer network, internet access facilities, computers and other school ICT equipment/devices or may commission an independent forensic audit.

1. DEFINITIONS

1.1. **ICT -** 'Information and Communication Technologies'

1.2. **School ICT -** School's computer network, internet access facilities, computers and other school ICT equipment/devices as outlined below.

1.3. **ICT equipment/devices –** Includes, but is not limited to, computers such as desktops, laptops, and tablets; storage devices such as USB and flash memory devices, CDs, DVDs and webcams. All BYO personal devices must meet all minimum specifications, *please refer to the Minimum Specification Sheet*.

1.4. **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 and is not considered to be in line with the School's values or is incompatible with a school environment. *This is intended to be inclusive of the definition used in the Films, Videos and Publications Classifications Act 1993.*

2. RESPONSIBILITIES RELATED TO PERSONALLY OWNED DIGITAL DEVICES (YEAR 7-12 ONLY)

2.1 The following things remain the responsibility of students and their parents or guardians:-

2.1.1 Ensuring the device is brought to school fully charged and functioning with a minimum battery life of six hours as set out in the *Minimum Specification Sheet*.

2.1.2 All repairs and maintenance.

2.1.3 Insurance and insurance claims.

2.1.4 Anti-virus, anti-spam, spyware, firewalls and off campus content filtering software.

2.1.5 Reasonable steps to secure devices and protect devices from theft whilst at school. The School will take no responsibility for any loss or damage to personal digital devices. (*Refer clause 2.2)*

2.1.6 Software and software related issues relating to things such as Microsoft Office, browsers, multi-media software etc. remain the responsibility of the owner.

2.1.7 Backups.

2.1.8 All device content, inappropriate or otherwise.

2.2 The School commits itself to the following responsibilities:-

2.2.1 To enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the internet or school ICT equipment/devices, where reasonably possible.

2.2.2 To work progressively with students and their families to encourage and develop an understanding of the importance of cybersafety through education designed to complement and support the *Use of Digital Devices and Cybersafety Agreement*.

2.2.3 To keep a copy of this signed *Use of Digital Devices and Cybersafety Agreement* on file.

2.2.4 To respond to any breaches in an appropriate manner.

2.2.5 To welcome enquiries from parents or students about cybersafety issues.

3. RULES TO FOLLOW WHEN USING ICT EQUIPMENT AND PERSONAL DIGITAL DEVICES AT SCHOOL

3.1 Whilst using a personal digital devices at school students **MUST:**

3.1.1 Use it for educational purposes as directed by a staff member.

3.1.2 Act responsibly and not use the device to find, create or send information that might be harmful, inappropriate or hurtful to anyone else.

3.1.3 Respect others when talking to and working with them online and never write or participate in online bullying.

3.1.4 Seek permission from individuals involved **before** taking photos, recording sound or videoing them (including all staff).

3.1.5 Seek written permission from individuals involved **before** publishing or sending photos, recorded sound or video to anyone else or to any online space.

3.1.6 Seek a staff member's permission before uploading any content to websites (e.g. blogs).

3.2 Only students with a completed Agreement on file will be allowed to access and use the School's Wi-Fi network.

3.3 Students must only log on with their own username and password and must not share this information with anyone else.

3.4 Students may bring their own personal digital devices such as tablets and laptops to school. All BYO devices brought to school must meet the minimum specification guidelines, *please refer to the Minimum Specification Sheet. (Years 7 to 12 Only)*

3.5 Whilst using the School's Wi-Fi network, computers or a personal digital device in school, students must **NOT:**

3.5.1 Eat or drink near computers or computer-related equipment.

3.5.2 Access, or attempt to access, inappropriate, age-restricted, or objectionable material.

3.5.3 Download, save or distribute such material by copying, storing, printing or showing it to other people.

3.5.4 Provide false or misleading information regarding their identity.

3.5.5 Provide ANY personal information about themselves or others to any third party without a staff member's implicit consent. This includes digital media.

3.6 Whilst using the School's Wi-Fi network, computers or personal digital devices in school, students **MUST:**

3.6.1 Only use software appropriate to the class being taught at any given time.

3.6.2 Allow access to their device by any authorised member of staff, at any time, for checking and compliance purposes.

3.6.3 Treat all computer equipment with the utmost of care at all times.

3.6.4 Ensure they have clean hands when using computer-related equipment.

3.6.5 Follow correct procedures when operating any type of computer equipment.

3.6.6 Not touch, tamper with, adjust, move, and attempt to fix or remove any computer or computer related equipment belonging to the School, unless they are instructed to do so by the staff member in charge.

3.6.7 Not make any kind of change, modification, adjustment, or attempt to fix any computer or computer resource belonging to the School.

3.6.8 Ensure all content on the device is appropriate to a school environment.

3.6.9 Not attempt to gain unauthorised access to the School's Wi-Fi network at any time for any reason.

3.6.10 Immediately report any inappropriate use of the internet to a staff member.

3.7 Failure to adhere to these requirements and any wilful damage to the School's computer network may result in disciplinary actions such as suspended use, expulsion, police involvement and possible restitution.

4. PRINTING/USAGE QUOTAS

4.1. All students have a set printing quota. If that the quota is exceeded due to inappropriate use, they may incur a charge in order to increase this quota.

4.2. All students have a set internet download quota. If the quota is exceeded due to inappropriate use, they may incur a charge in order to increase this quota or their usage may be suspended.

5. SOCIAL NETWORKING

When using social network sites such as Facebook, Twitter and other sites, where freedom of expression is possible, respect for the school and its community must be demonstrated. Students must not at any time participate in:-

5.1. Targeting any BHCS student or staff member with perceived negative intent.

5.2. Identifying other students or staff as being part of BHCS.

5.3. Undermining the name and/or good work of the School.

5.4. Using derogatory speech when referring to anything related to BHCS.

5.5. Misrepresenting the school and the members of its community.

6. HARASSMENT AND CYBERBULLYING

6.1. Students must not participate in any form of conduct, whether digital, written, verbal or physical, that unreasonably interferes in another's participation in, or enjoyment of, school or school sponsored activities. This includes, but is not limited to the sending or posting of inappropriate and hurtful e-mail messages, instant messages, text messages, digital pictures/images, or website postings including blogs. All reports of harassment will be investigated fully.

6.1.1. For the purpose of this policy both harassment and cyberbullying will be deemed as consistently and continually intimidating or attempting to intimidate others by any means or methods including:

6.1.1.1. Threatening or terrorising

6.1.1.2. Taunts or teasing

6.1.1.3. Name-calling or put-downs

6.1.1.4. Discriminatory actions

6.1.1.5. Extortion

6.1.1.6. Exclusion

6.2. Neither the school's network nor the broader internet (whether accessed on campus or off campus, either during or after school hours) may be used for the purpose of harassment.

6.3. Neither the school's network nor the broader internet (whether accessed on campus or off campus, either during or after school hours) may be used for the purpose of harassment.

6.4. All forms of harassment in cyberspace are unacceptable. Sending threatening messages through electronic means may be criminal in nature. It is a criminal offence to use a personal digital device to menace, harass or offend another person and almost all calls, text messages and emails can be traced. *Please refer to the Cybercrime Act 2001*.

6.5. Typically, the School will not be involved in the resolution of any cyberbullying that occurs outside of school, unless it creates a reasonable threat, which will interfere with day-to-day activities at school.

7. CONSEQUENCES OF MISUSE OF DIGITAL DEVICES

7.1. Failure to comply with the conditions in this agreement may result in computer privileges being withdrawn for a period of time. Reinstatement will be at the discretion of the relevant staff member or co-ordinator.

7.2. Any use of personal electronic devices which breach this policy may result in the device being confiscated for a given period of time.

7.3. Continued breaches of the conditions set out in this policy, may result in further disciplinary action up to and including suspension, isolation or expulsion from school and possible police involvement.

7.4. In some cases, misuse of personal digital devices can constitute a criminal offence and will be referred to the Police. *Refer to the Cybercrime Act 2001*.

Have a look at the video material for primary students at
http://www.cybersmart.gov.au/cyberquoll/index.html
This site also has a helpline for Kids: Tel 1800 551 088
You can read more on how to stay Cybersafe at: www.cybersmart.gov.au

Adapted for Belgrave Heights Christian school from the www.cybersafety.gov.au website.