CHILD SIDE PLAYGROUP AND SCHOOL FOLLOWS CHILD PROTECTION AND PROTECTIVE BEHAVIOUR PROCESSES

Internet and Electronic Devices Policy

Introduction

Recommendation 6.22 of the *Royal Commission into Institutional Responses to Child Sexual Abuse* called for the eSafety Commissioner to oversee the development of a framework and resources that support schools in creating child-safe online environments.

Child Side Playgroup and School (CSS) provides electronic communication facilities for its children and employees for educational and/or administrative purposes. By its nature, electronic communication is a fast and informal way of communicating. Purposeful and thorough oversight in relation to the management of infrastructure and resources are essential to maintain child-safe online environments that are positive and supportive places for all children.

CSS is committed to providing and ensuring child-safe online environments through well-articulated, whole school approaches which includes clear direction as to the appropriate use of the internet and electronic devices by all School Community members.

CSS recognises that a child-safe organisational focus not only provides for the safety of children, but it also helps to safeguard the school, staff, and others from going in a direction that could lead to legal action, a loss of reputation and/or put the school at financial risk.

Scope and Application

This policy applies to all School Staff (paid/unpaid), parents, children, volunteers, practicum teachers, work experience students, Governing Council members, and visitors of CSS .

The use of the word child/children in this policy refers to students in the context of the school environment.

The use of the word Educator/Educators in this policy refers to registered teachers in the context of the school environment.

Related Legislation/Guidelines

- Criminal Code Amendment (Cyber Predators) Act 2006
- Copyright Amendment (Digital Agenda) Act 2000
- Copyright Amendment (Moral Rights) Act 2000
- Fair Work Act 2009
- School Education Act 1999
- School Education Regulations 2000
- Teacher Registration Act 2012
- Teacher Registration (General) Regulations 2012
- Telecommunications (Interception and Access) Act 1979
- Telecommunications Act 1997
- Equal Opportunity Act 1984 (WA)
- Privacy Compliance Manual - National Catholic Education Commission and Independent Schools Council of Australia
- School Education Act 1999

- Privacy Act 1988
- National Child Safe Organisation Principles
- Australian Government eSafety Commissioner – eSafety Education Resources

Related Policies/Guidelines/Documents

- Anti-Discrimination and Harassment Policy
- Assessment and Reporting Policy
- Anti-Bullying Behaviour Policy
- Child Protection Policy
- Code of Conduct – ECC and MCC (K-6)
- Code of Conduct – YAC (7-10)
- Code of Conduct – School Staff
- Code of Conduct – School Staff Guidelines and Agreement
- Code of Conduct – Governing Council
- Code of Conduct – Parent/Guardian
- Staff Use of Social Media Policy
- Use of Children's Photographs and Video Images Policy
- CSS Curriculum Overview
- Concerns, Complaints and Disputes Policy
- Whistleblower Protection Policy
- Curriculum Evaluation Policy
- Guiding Children's Behaviour Policy
- Privacy Policy
- Use of Children's Photographs and Video Images Policy
- Risk Management Policy and Risk Management Register

Definitions

Cyber bullying
Bullying online, or 'cyberbullying', is when someone uses the internet to be mean to another person, so they feel bad or upset. No one deserves to be bullied online. In short: Bullying that happens online can harm the mental and physical health of the person targeted. eSafety Commissioner

Policy Statement

At CSS we see computers and other digital devices, as another tool for learning. As with other tools, the computer, and other digital devices, need to be used selectively and for the appropriate job, with adult assistance and interaction with child safety and welfare being a primary consideration.

CSS acknowledges that competency and understanding ICT (Information Communication Technology) is a critical competency in contemporary education.

Computers and other digital devices (including mobile phones) will at any time, be used for a specific purpose or reason, integrated with children's current learning experiences and for authentic purposes as expressed by children and adults.

CSS maintains school online infrastructure, equipment and policy which is designed to ensure safety for all users and protects the school against cyber-attacks and privacy and data breaches. This strategy includes the monitoring and the viewing of data stored or transmitted using the school's facilities.

CSS maintains clear and shared procedures and guidelines for employees (paid and unpaid), and Governing Council members as to their responsibilities around:
- the use and access of CSS resources including online access, and
- the use of their own devices including mobile phones.

CSS maintains clear and shared procedures and guidelines for children as to their responsibilities around the use and access of CSS resources including online access.

Policy Review

All policies are reviewed and amended in accordance with the *CSS Policy on Policies* and the *CSS Policy, Guidelines, Procedures and Frameworks Register*.

This policy and associated guidelines will be reviewed every two years; provided that an earlier review is undertaken whenever a matter or other information becomes evident regardless of indicators or not, there has been a policy or procedural failure.

Appendices

Appendix 1	Internet and Electronic Devices Guidelines and Procedures
Appendix 2	*Child Side Playgroup and School Child Phone Agreement*
Appendix 3	Security Devices and Software Information

Version Management

VERSION	DATE REVIEWED	DATE RATIFIED	CHANGES MADE	AUTHOR OF CHANGES	NEXT REVIEW DATE
1	June 2011	10/8/2011	Minor	LO	
2	June 2014	25/6/2014	Name changes	KM	
3	Feb 2015	25/2/2015	Year level changes e.g. 3-7 to 3-6	KM	
4	March 2015	27/5/2015	In reference to cyber safety and physical environment set up	Staff on SDD day	
5	Dec 2015	9/12/2015	Actions in relation to children's safety Commissioner added	KM	
6	Oct 2018	20/3/2019	Update format to include related legislation, policies, and procedures` Include YAC BYOD requirement	LF & KM	Term 1 - 2022
7	Sept 2021	20/07/2022	Changed title to include devices and content including reference to usage by staff and children in statement and procedures. Added information regarding school devices, safety, and storage.	LF	Term 3 - 2025
8	Nov 2023	15/11/2023	Added reference in procedures to 3 school iPads allocated to clusters for educators to take images and videos of children for evidence of learning	LF	Term 4 - 2026
9	May 2024		Minor formatting Added eSafety links and resources appropriate for online safety teaching and learning. Included a protective behaviours statement in the policy introduction. Added additional procedures to the guidelines to expand responsibilities of stakeholders. Added a Child Phone Agreement proforma	JM	Term 2 2026

Internet and Electronic Devices Guidelines and Procedures

Our Philosophy

Despite the current popular high regard and urgency for children to use computers from an early age, there is contradictory evidence to the long-term benefits for children's learning (see reference list below for starters). Many highly regarded educational researchers and theorists such as Jane Healy and Howard Gardner are questioning the way we use computers in schools and their value for money (including the high need for maintenance, constant updating, commercial software products and human resources attached to them), given all the other resources needed to create a stimulating, multi-sensory learning environment indoors and outdoors for children. We do not wish for computers to come at the expense of other more relevant tools and resources and learning experiences offered to children, especially in the early childhood phase of schooling.

At Child Side Playgroup and School, we see computers as another tool for learning, just like a hammer or a paintbrush and as with other tools, the computer needs to be used selectively and for the appropriate job with adult assistance and interaction.

It is not to be used to keep children busy playing games or surfing the internet for no legitimate reason. Children's time is far better used to interact with others, interact with books, explore the outdoors and tinker with other materials and resources, especially in the early childhood phase of schooling. Computers are of high interest and motivation for children, but careful observation can show children merely pushing buttons and playing reactive games, rather than reading, thinking, or processing information or using any 'habits of mind' (such as the concern for evidence using their 'filters'; finding patterns or relationships; seeing multiple perspectives; hypothesizing and finding a range of possibilities; asking themselves what does this information/evidence matter and to whom? Or how they can use this information/evidence/process to express, share, clarify, confirm, contradict, communicate what they already know or have found out?)

Computers are an amazing open-ended resource/tool when used wisely and with deliberation, purpose, and care. Adult interaction and interest is essential for demonstrating functions and purposes/possibilities of computers and modelling 'habits of mind' and developing 'filters'. Research into brain development cautions against the wide-spread use of the internet as a means of collecting information for children in the early years and even middle years of schooling. Adult interaction is essential, even with the appropriate commercial 'filters' that schools use to censor certain things available on the internet for children.

All parents/guardians are encouraged to think carefully about their own personal computer/play station/game policy at home and to regularly ask themselves what their children are learning (especially what are the 'messages' for children behind many of the games). They are also encouraged to regularly interact with their children when they are on the computer or play station at home and to help their children develop 'filters' to understand and process these 'messages' and ideas. Parents are encouraged to question the intent behind the programme or game and to consciously decide whether they think it is appropriate for their child/ren, (children will show a high interest and motivation regardless of the content, intent or message behind the game or programme, therefore it will need to be the adult's decision with appropriate discussion with the child.)

Child eSafety Curriculum

Children need to be explicitly taught protective behaviours and codes of conduct while using the internet both at home and school. These need constant revisiting and regular monitoring (especially as their brains mature and their interests change). Children need to understand the limitations of the internet as well as its 'global' value.

The CSS *Protective Behaviours Curriculum Plan* is implemented at each Cluster level (ECC, MCC and YAC)which is developmentally appropriate and integrated with the *Keeping Safe Child Protection Curriculum* and embedded in the *CSS Curriculum Map*. This work is supported by the resources provided by the eSafety Commissioner to provide embedded and purposeful eSafety best practice.

The eSafety Commissioner provides *resources* that was developed in response to the *Royal Commission into Institutional Responses to Child Sexual Abuse,* that supports schools in creating child-safe online environments and to address bullying and cyberbullying.
eSafety's Best Practice Framework for Online Safety Education establishes a consistent national approach that supports education systems across Australia to deliver high quality programs, with clearly defined elements and effective practices. The Framework's implementation guide helps school leaders, educators and program providers use the Framework to design, deliver and review online safety education. It includes relevant links to the *Toolkit for Schools*, eSafety's classroom resources, the Australian curriculum, and existing policies and frameworks.

The Framework is organised by five 'elements'.
They are the evidence-based overarching principles that should be used to determine whether best practice is being applied in a program.
- Element 1 – Students' rights and responsibilities
- Element 2 – Resilience and risk
- Element 3 – Effective whole-school approaches
- Element 4 – Integrated and specific curriculum
- Element 5 – Continuously improved through review and evaluation

Each of the five elements has associated 'effective practices'. A total of 22 effective practices are defined within the Framework.

The *Toolkit* should be used in conjunction with eSafety's *Best Practice Framework for Online Safety Education*.

https://www.esafety.gov.au/educators/best-practice-framework

https://www.esafety.gov.au/educators/toolkit-schools

School Devices – Safety and Storage.

The school ITC contractor provides up-to-date advice, support, and services to assist in the provision and monitoring of the most appropriate devices, technologies, and security for the school setting.

Children - Devices

CSS has a lockable ITC cabinet in the MAG building for safe storage of all school owned and leased devices.

School Laptops and Tablets are available for children to use under the direction of the Continuity and Cohesion Educator (CCE) . Children are required to sign devices in and out of the allocated log book each time they are used.

All laptops have firewall and network protection, and students have access through a student share drive that is monitored by the school ITC contractor.

The Childrens' physical learning/working environment will be set up so that device screens are visible to Educators at all times. Computers will always be used in public places and in an open and transparent manner whereby cyber safety can be monitored by several adults. This applies to anyone on the school site.

School Staff - Devices

One school iPad has been allocated to each CCE, for the sole purpose of recording photographs and video images of children as evidence of learning. Companion Educators (C E) and Education Assistants (EA) will also have access to the iPads however, the children are not permitted to have use of these iPads. For safety, security, and privacy reasons the CCE will download the images from the iPads to the school server on a regular basis during the term.

Administrative staff are issued with a school computer for the purposes of carrying out their duties.

All School Staff bring their own devices for the purposes of carrying out their duties. These devices are provided with firewall and network protection as well as upgraded commercial level device protection if required. All staff (except relief teachers, practicum teachers and work experience students)have access through a *CSS shared drive* that is monitored by the school ITC contractor. All Staff are provided access to appropriate parts of the portal relevant to their role.

All School staff are issued with a dedicated school email address for the purposes of carrying out their duties and for school communication and is not to be used for personal purposes.

School Staff must not save or store any school related information on their personal devices including their phone.

School staff must not use the School's computer systems for personal reasons or to access social media, unless this access is for teaching, pastoral care, administrative or educational purposes and the employee has the permission of the Co-Principals.

The physical learning/working environment for all Staff will be set up so that device screens are visible to other staff members at all times. Computers will be always used in public places and in an open and transparent manner whereby cyber safety can be monitored by other adults. This applies to anyone on the school site.

The use of online programs and apps to support teaching and learning, require careful selection and discussion amongst Educators towards their intent, use and purpose. Educators should not use any program or app without discussion with the Co-Principal (Senior Educator).

Governing Council Members - Devices

All Governing Council (GC) Members bring their own device for the purposes of carrying out their duties.
All GC Members devices are provided with firewall and network protection as well as upgraded commercial level device protection if required. All GC Members have access to a *Child Side Sharepoint for GC* files that is monitored by the school ITC contractor.

GC Members must not save or store any school related information on their personal devices including their phone.

GC Members must not use the School's computer systems for personal reasons or to access social media unless the access is for educational, administrative, or professional learning purposes and the GC Member has the permission of the GC Chair.

Use of Computers by Children

Children will only use computers with adult knowledge and supervision.

Children in the Young Adolescent Cluster (YAC) have their own laptops in accordance with our BYOD requirements. The use of their computer is regularly checked, and any safety issues discussed with the children by their Educator.

Children are required to negotiate with adults and offer their evidence for choosing the computer as the most appropriate tool for their task (with help and support from adults). As part of this process, children may be required to draw, write, plan, discuss their idea/reasons before using the computer for their next stage to collect data/information, confirm, clarify, or contradict ideas/evidence to provide multiple perspectives and alternatives/possibilities.
This is part of the learning process of 'theory-repair' where children can use the computer/internet/emails to help them form/reform/deepen/modify their ideas and theories. This is an extremely complex process with which children will need adult guidance, support, and interest.
Afterwards children may also be required to 'do' something with the idea or 'evidence'/information they sourced using a computer/the internet, such as set up an experiment, design and create something, write, draw, discuss, display, print photos for the journals….

Children will be shown the appropriate computer skills and processes when they ask or when the Educator sees a need or when it is deemed developmentally appropriate by the Educator. Word processing skills can be learnt early; however, consideration should be given as to the reason and its relevance. Why expect children to do something today with difficulty that they will 'master' much easier and quicker when they are ready later on?

Adults can and should assist children to be thinkers by regularly and explicitly modelling and discussing their thoughtful processes and conscious decisions about computers and electronic devices and their use.

Notification of a Cyber Bullying Complaint

The Office of the eSafety Commissioner has a responsibility is to receive and manage complaints/ regarding cyber bullying.
In the event that a cyber bullying complaint is made to the 'Children's eSafety Commissioner' about CSS or a CSS child, employee or Community Member, there is a process that must be followed by the school. This is explained in the following excerpt :

'The Office of the Children's eSafety Commissioner – *resolving complaints with schools'*

What information we will give you?

When we notify of a complaint to a school principal, we may provide information about:

a) The name of the student who is the target of the cyber bullying.

b) A summary of the cyber bullying material.
c) Suggested options to help resolve the complaint in accordance with your school policies.
d) Action taken by us to date with respect to the complaint.

We will also advise you of any conditions that apply to the use of the information supplied by us (see below).

What actions should schools take?

If we notify you about a cyber bullying complaint concerning children in your school, you can help resolve the complaint by undertaking to do the following (to the extent that you are capable of doing so):

a) Acknowledge receipt of the notification within 24 hours to an email address provided by us.
b) Inform us of the types of actions the school proposes to take and the time period for that action to be taken by email within 5 working days of the notification.
c) Meet any conditions placed on information that has been disclosed.
d) Inform us of the outcomes of the action you have taken within 3 weeks from receipt of the notification.
e) Talk to us if you feel that you are unable to resolve the complaint and/or that you have a serious concern that the bullying will continue so we can discuss any further assistance we may be able to provide.

Disclosure of information – conditions

When we disclose information to you, amongst other things we may ask you to:

1. Only discuss the information with the children involved and – with the student's consent – their parents or guardians.
2. Only disclose the information to third parties with the consent of the affected children or as required by law.
3. Comply with applicable privacy laws and policies in relation to the personal information disclosed.

Acceptable Use of Mobile Phones at School

CSS has an established and consistent approach for the use of mobile phones in school that is well advertised and managed and will assist in preventing many of the negative consequences the use of these and associated technologies can present.

Use of Mobile Phones by Children

Children are **not** to bring a mobile phone to school, school events nor on excursions, camps, or any other extra-curricular activity.

Parents/Guardians are asked to not send a mobile phone with their child to school and to regularly check that their child/children do not bring a phone to school.
If a mobile phone is brought to school without the appropriate permission, the child will be asked to take their device to the office where it will be given to a Co-Principal and stored for the school day. If the phone is not relinquished by the child, then the Parent/Guardian will be contacted to come to the school to collect the phone. In this event, consideration will be given by the Co-Principals as to any breach of the Code *of Conduct* by both the Child and the Parents/Guardians.

CSS has straight forward and well-advertised processes and procedures for Parents/Guardians to be able to contact their Child during the school day if necessary.

If a Parent/Guardian requires a child to bring a mobile phone to school for a one-off reason, the Parent/Guardian should speak with a Co-Principal prior to the phone arriving at school. The phone is to be given to a Co-Principal at the start of the school day where it will be kept in the office. The phone can be collected by the child or their Parent/Guardian at the end of the school day. If there is an ongoing (and reasonable) need for a child's phone to be at school, there must be a *CSS Child Phone Agreement* negotiated (see the agreement form attached to this policy).

It is acknowledged that some children may require a mobile phone to be used in school as a special needs tool for educational assistance. In this instance, the child will need approval from the Co-Principal (Senior Educator), their CCE and their Parents/Guardians to use the mobile phone in the classroom. If there is an ongoing (and reasonable) need for a child's phone to be at school, there must be a *CSS Child Phone Agreement* be put in place (see the agreement form attached to this policy).

If a Child's mobile phone is approved using the appropriate processes, the following conditions apply :

Responsibility.

- Children who bring a mobile phone to school will be held responsible for the use of that phone by themselves or anyone else.
- The child's phone should not be used by any other person other than themselves.
- If a child's phone is used by someone else, they must immediately inform their CC Educator or the Co-Principal.
- Permission to have a mobile phone at school/while under the school's supervision is contingent upon the Co-Principals' and the Parent/Guardian permission. Permission may be revoked by either party at any time.
- It is the child's responsibility to follow all of the conditions of the *Child Phone Agreement*. The child's Educator or the Co-Principals are not responsible to enforce the conditions.

Acceptable Uses.

- Mobile phones should be switched off during classroom lessons unless specifically allowed by the CC Educator.
- Parents/Guardians may request that their child keeps a mobile phone switched on. This request will be handled on a case-by-case basis and should be directed to the Co-Principals and while the phone agreement is being negotiated.

Unacceptable Uses.

- Unless express permission is granted to the contrary, mobile phones must not be used in class for any reason.
- Mobile phones should not disrupt classroom lessons by ringing or beeping.

Consequences.

Breaches of a phone agreement may result in the relinquishing of the child's phone, rescinding their permission to bring a phone to school or some other consequences determined by the school including breach of Code of Conduct.

Theft or damage.

- Children are required to mark their mobile phone clearly with their names.

- Mobile phones which are found in the school and whose owner cannot be located should be handed to a CC Educator or a Co-Principal.
- The school accepts no responsibility for replacing lost, stolen, or damaged mobile phones.
- It is strongly advised that students use access security on their mobile phone. Students must keep their password/pin numbers confidential.

Use of Mobile Phones by School Staff (paid/unpaid)

Mobile phones are required to be used by staff for a variety of purposes including:

- recording observational and education data,
- communication and emergency purposes as well as updating parents on the health status of children,
- School communication between staff during the school day, and
- to receive school communications via the school communication app.

The following conditions apply for the use of mobile phones by School staff:

Responsibility.

- School Staff who bring a mobile phone to school will be held responsible for the use of that phone by themselves or anyone else.
- If a Staff members' phone is used by someone else without their permission, they must immediately inform the Co-Principals.

Acceptable Uses.

- School Staff should only use their mobile for the purposes as stated above,
- School Staff should use their mobile phone in line with other CSS policy including *CSS Code of Conduct – School Staff*, *CSS Social Media Policy*, and *Use of Children's Photographs and Video Images Policy*.

Unacceptable Uses.

- Unless express permission is granted to the contrary, mobile phones must not be used at school for personal reasons.
- Mobile phones should not disrupt classroom lessons by ringing or beeping.

Consequences.

Breaches of mobile phone use may result in consequences determined by the school including breach of Code of Conduct.

Theft or damage

- Mobile phones which are found in the school and whose owner cannot be located should be handed to the Administration Assistant, a CCE or a Co-Principal.
- The school accepts no responsibility for replacing lost, stolen, or damaged mobile phones.
- It is strongly advised that all school staff use access security on their mobile phone. All school staff must keep their password/pin numbers confidential.

take a walk on the Child Side Playgroup and School

CHILD SIDE PLAYGROUP AND SCHOOL FOLLOWS CHILD PROTECTION AND PROTECTIVE BEHAVIOUR PROCESSES

Child Side Playgroup and School Child Phone Agreement

I request that my Child _____ has permission to bring a mobile phone to school for the following reason/s :

☐ The phone is in transit between homes. It is not required to be used at school, just held for safekeeping in the office during the school day. It will be handed to an agreed CSS Staff member at the beginning of the school day.

☐ My Child requires their mobile phone to be used in school as a special needs tool for educational assistance. *(These needs should be discussed and understood by the Co-Principals and the Educator. If this is not a recommendation from the child's Educator, it is preferable that there be a therapist/health professional recommendation/plan provided to assist the Educator support this request)*

☐ My Child requires their mobile phone to be used in school as a special needs tool for mental health support. *(These needs should be discussed and understood by the Co-Principals and the Educator. If this is not a recommendation from the child's Educator, it is preferable that there be a therapist/health professional recommendation/plan provided to assist the Educator support this request)*

☐ My Child requires their mobile phone to be used in school …

_____

_____

_____

(This reason should be discussed and understood by the Co-Principals and the Educator)

The following conditions apply when a Child's phone is brought to school:

Responsibility.

- Children who bring a mobile phone to school will be held responsible for the use of that phone by themselves or anyone else.
- The child's phone should not be used by any other person other than themselves.
- If a child's phone is used by someone else, they must immediately inform their CC Educator or the Co-Principal.
- Permission to have a mobile phone at school/while under the school's supervision is contingent upon the Co-Principals' and the Parent/Guardian permission. Permission may be revoked by either party at any time.
- It is the child's responsibility to follow all of the conditions of this agreement. The child's Educator or the Co-Principals are not responsible to enforce the conditions.

Acceptable Uses.

- Mobile phones should be switched off during classroom lessons unless specifically allowed by the CC Educator.

- Parents/Guardians may request that their child keeps a mobile phone switched on. This request will be handled on a case-by-case basis and should be directed to the Co-Principals and while the phone agreement is being negotiated.

Unacceptable Uses.

- Unless express permission is granted to the contrary, mobile phones must not be used in class for any reason.
- Mobile phones should not disrupt classroom lessons by ringing or beeping.

Consequences.

Breaches of a phone agreement may result in the relinquishing of the child's phone, rescinding their permission to bring a phone to school or some other consequences determined by the school including breach of Code of Conduct.

Theft or damage.

- Children are required to mark their mobile phone clearly with their names.
- Mobile phones which are found in the school and whose owner cannot be located should be handed to a CC Educator or a Co-Principal.
- The school accepts no responsibility for replacing lost, stolen, or damaged mobile phones.
- It is strongly advised that students use access security on their mobile phone. Students must keep their password/pin numbers confidential.

Agreed exceptions/additional conditions to this policy.

The following exceptions/additional conditions have been agreed.

_____

_____

_____

_____

_____

Parent/Guardian permission and acknowledgement

I have read and understand the stated conditions of the use of my Child's mobile phone at Child Side Playgroup and School.

I understand that this agreement will be kept on file at the school and that the details may be used, and shared with a third party, to assist identify a phone should the need arise.

I understand that my child will be responsible for ensuring that the mobile phone is used appropriately and as agreed while at school.

I understand that my child may face consequences for breaches of this agreement.

Parent/Guardian name (print) _____

Parent/Guardian signature _____

Date _____

My Phone Agreement Acknowledgement

I have read and understand the stated conditions of use of my mobile phone at Child Side Playgroup and School.

I understand that this agreement will be kept on file at the school and that the details may be used, and shared with a third party, to assist identify a phone should the need arise.

I understand that I will be responsible for ensuring that my mobile phone is used appropriately and as agreed while at school.

I understand that I may face consequences for breaches of this agreement.

Child name (print) _____

Mobile phone number _____

Child signature _____

Date _____

Co-Principal Signature _____

Educator signature _____

Date _____

Unless otherwise stated, this agreement will cease on the last day of the school year, unless this agreement has been ceased, changed, or cancelled before this time.

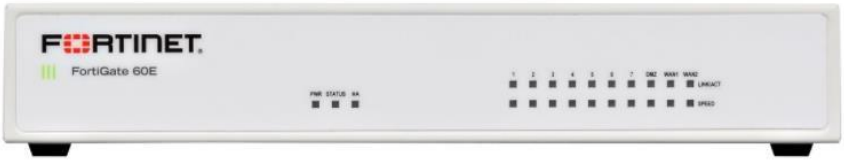
A copy of this signed agreement should be provided to the Child/Parent/Guardian.

Child Side Playgroup and School Security Devices and Software Information

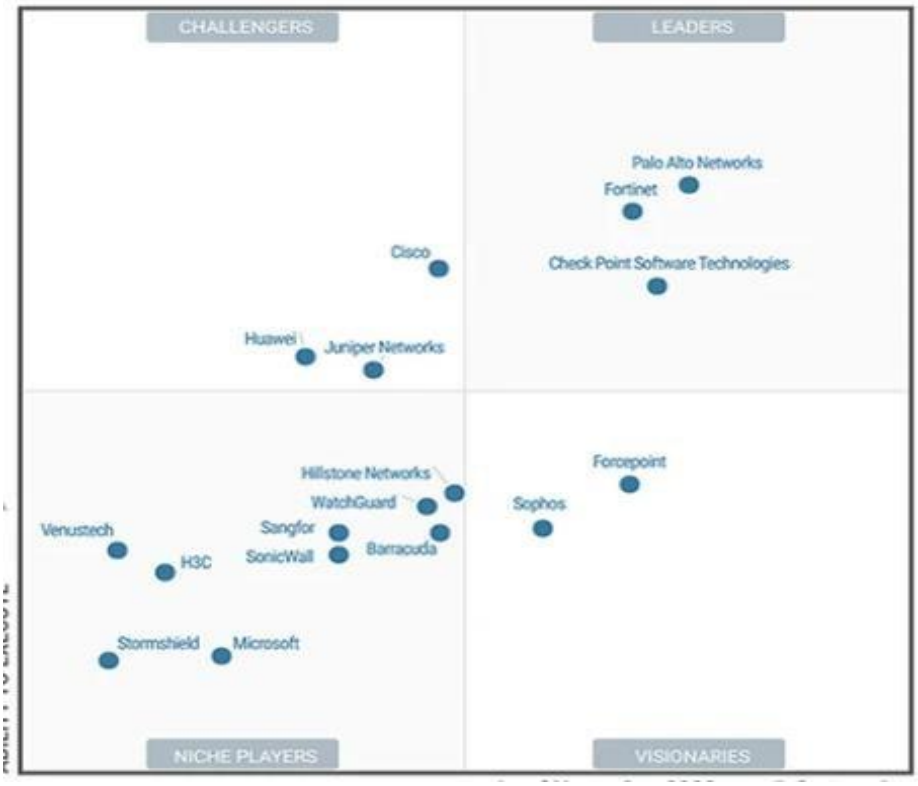
CSS currently has the following security devices and software in place to help prevent a cybersecurity attack, data, and privacy breaches and to protect students and school staff from external exposures.

1. Enterprise Grade Fortigate Firewall Enterprise
2. Garde Comodo Anti-Virus
3. Windows 2019 domain network.

1. Fortinet Fortigate Firewall



Fortinet is regarded as one of the top firewalls manufactures in the world and has achieved the right top quadrant in the most recent Gartner report (June 2021) for Leaders in firewall technology.



With the enhanced DPI (Deep Packet Inspection) license content can be scanned to ensure students are not able to access prohibited content while using the school's infrastructure. This is very important in today's world.

2. Anti-Virus

BizLinQ Anti-Virus (Comodo) is the only true product that stops viruses and any other unwanted malicious malware/viruses from entering corporate systems. With its patented containment technology, it can truly stop viruses in its tracks. Comodo believes its technology is different from its competitors, in that, they deliver prevention-based solutions vs detection based products.

3. Windows 2019 Server Network

Child Side Playgroup and School has a fully functional Windows 2019 server environment. There are 2 x servers running on a single host. The first server call the Windows Domain Controller is responsible for enterprise level security, providing security not only to corporate data, but also providing security to connect devices attached to the corporate network. Student data and teacher data is also securely saved onto the server in folders with security permissions assigned to each folder according to requested requirements.

The second server a RDS (Remote Desktop Server) provides a Windows 10 style virtual desktop which provides staff and possible Governing Council members access to the school system and data remotely. It also provides Apple based users with the same set of applications as any Windows based user for total compatibility across the environment. Remote access to the RDS server is via the firewall when working remotely using either the Fortinet client or a secured SSL browser connection.