E-SAFETY POLICY

This policy describes the rights and responsibilities of Hopes and Dreams' staff using Information and Communications Technology (ICT), such as computers, telephones and Internet applications. It explains the procedures you are expected to follow and makes clear what is considered acceptable behaviour when using them.

These facilities are a vital part of Hopes and Dreams' business and should be used both appropriately and in the best interests of Hopes and Dreams.

This policy forms part of your employment contract with Hopes and Dreams and is available in the Employee Handbook in the Staff Room.

Named E-Safety Leads
The Designated Safeguarding officer at Hopes and Dreams is Cornelia Harrison (Lead) and the Deputy Safeguarding Officer is Lek Teo. If you have any concerns about E-Safety or safeguarding of children, in relation to using ICT equipment, you should contact the Designated Safeguarding officer or the Deputy Safeguarding officer in their absence.

Health and Safety
You are encouraged to share any concerns about the equipment you are using with your manager, either at the time of completing a risk assessment or at any other time a concern arises.

Security
All information on Hopes and Dreams' network is confidential with some areas restricted for general access. Any attempt, whether successful or not, to gain unauthorised access to, or to tamper with, any computer system, software or installation, including the telephone system, will be regarded as gross misconduct. This includes the malicious deletion or alteration of documents created by you or others in the course of your duties. You may also be liable to prosecution under the *Computer Misuse Act, 1990*, even where no damage results from your action.

Equipment and Safekeeping of Equipment
All computer equipment is installed professionally and meets health and safety standards. It is the responsibility of the ordinary user to take care of any item of equipment allocated to them and advise the office if the equipment is found to be faulty. If it is determined that any failure of equipment is due to improper use or care you may be required to contribute to the cost of any replacement.

File Management
All electronic data should be stored on Hopes and Dreams' network (e.g., on the U:/ drive) and not on local or removable drives. Items stored on local drives (for example, the PC or laptop's C:/ drive or desktop) will not be backed up, and could therefore be irretrievably lost in the event of a device breaking. It is not permitted for work-related files to be stored on your own home PC, laptop or any other personal removable device/s, such as flash or hard drives, mobile phone storage, etc. It is prohibited for personal telephones and/or any other

personal devices to be connected to Hopes and Dreams computers and network systems at any time.

Work Email
As email is not a totally secure system of communication, and can be intercepted by third parties, external email should not be used in relation to confidential transactions. Email messages do not cease to exist when you delete them from your terminal; they remain on Hopes and Dreams' hardware and can be retrieved if required by Hopes and Dreams. The content of emails may be relevant to legal action against Hopes and Dreams and, therefore, emails may have to be disclosed. Messages sent on the email system for business purposes should comply in both form and content of language used and to the high professional standards applied by Hopes and Dreams to all other written forms of communication.

Internet Access
Hopes and Dreams reserves the right to monitor employees' Internet usage, and fully investigate reasons for its use. The company reserves the right to retain information that it has gathered on employees' use of the Internet for a period of one year. Employees must not use Hopes and Dreams' Internet facilities to visit, bookmark, download material from, or upload material to, obscene, pornographic, or otherwise offensive websites. This could infringe copyright, incur expense for the organisation, or expose it to criminal penalties or liability for harassment or defamation. Such use constitutes misconduct and will lead to disciplinary action, up to and including summary dismissal in serious cases. The final decision on appropriateness of a site, or appropriate Internet access, remains with the Senior Management Team. Each employee has a responsibility to report any Internet or email misuse. By not reporting such information, the employee will be considered to be collaborating in any misuse. All employees can be assured of confidentiality when reporting misuse.

Personal Use of the Internet
Any use of Hopes and Dreams' electronic communication systems (including email, Internet, Wi-Fi and telephones) for purposes other than the duties of your employment is a discretionary privilege given to employees by Hopes and Dreams. Use of the computers outside of your working hours is permissible, if it has been agreed by a manager, and providing it does not interfere with colleagues' work or infringe any of the acceptable use criteria. If any other member of staff needs to use the PC/Internet for work-related matter/s you will be required to vacate the computer you are using for your personal needs immediately. Use of the Internet or the Wi-Fi network for personal reasons during working hours is not permitted.

Personal Email
Outside of working hours (before/after work, lunch breaks) you are permitted to use the Internet on the Nursery School Office/Balcony Area for personal reasons, such as checking emails. However, please note that you are required to log out/off from any applications immediately after you have finished using them.

Use of iPads
Hopes and Dreams uses a website-based system called My Montessori Child for administrative and record-keeping purposes, including taking the attendance register, making text-based and photographic records of children's activities, recording contact information, planning lessons, reviewing children's progress, and compiling statutory Department for Education reports. Text, data and photographs are uploaded to My Montessori Child servers by teachers using Internet-connected Apple iPads within the setting. Text, data and photographs are stored remotely on My Montessori Child's online servers and are protected by industry-standard Internet security procedures including encrypted transmission, teacher-access PINs, access-device registration and physical protections.

(Further details about system security are shown on the My Montessori Child teachers' website under Children > Help > System security.) The system administrator of My Montessori Child and the software developer of My Montessori Child, who have access to the children's data and photographs on a need-to-know basis, have been subject to an Enhanced Disclosure Criminal Records Bureau (CRB) check (Disclosure numbers 001382556238 and 001425881405). My Montessori Child is registered in accordance with the Data Protection Act with the Information Commissioner's Office (Registration Z3311745).

Physical storage of photos on iPads
The system is designed so that text, data and photographs are saved directly to My Montessori Child's remote, secure web servers. This means that no photos nor any text or data are stored on the iPad itself. All photos must be deleted weekly by Friday. IPads are not allowed to be taken off the premises.

Physical location of iPads in the setting
When not in use the iPads are stored securely in designated areas within the class rooms. No iPad may be used in toilets or nappy-changing areas without at least two teachers being present. Teachers must behave responsibly with iPads as pieces of delicate electrical equipment, protecting them from damage and ensuring they pose no physical risk to children.
IPads are not allowed to be taken off the premises.

Uploading of photos to the Internet
Photos taken with the iPad are never uploaded to any part of the Internet except to My Montessori Child's secure servers. For example, no photo of any child or group of children on the iPad may be e-mailed, posted to Facebook, tweeted on Twitter, or pinned to Pinterest. Parent requests to e-mail photos from an iPad are always refused for security reasons. In order to ensure that no photos are being uploaded, e-mail 'sent' lists and web histories on the iPad are never cleared so that they may be checked by the Management team.

iPad Restrictions
All iPads used in the setting have PIN-protected 'Restrictions' on what web content, applications and functions may be used. Specifically, in Settings > General > Restrictions, the following restrictions are applied:
- In-App Purchases is 'Off'
- Allowed Content is set (using UK ratings) as follows: 'Clean' Music & Podcasts, 'U'-certificate movies, 'CAUTION' TV Shows, 'Restricted' Books, and '4+' Apps
- Require Password is set to 'Immediately'
- In the Game Centre section, Multiplayer Games are 'Off'.

Use of the Internet in the Nursery School Snowdrops and Rainbow Rooms
The Internet facility provided for both the Snowdrops and Rainbow classroom computers are only available for educational purposes in connection with the Hopes and Dreams children's curriculum needs. Children should never be allowed to use the Internet in the setting without adult supervision.
**Personal use of the computers in both the Snowdrops and Rainbow classrooms is not permitted at any time.*

Website and Social Networking Restrictions
**It is prohibited at all times for offensive content and/or viruses to be viewed and/or downloaded on our network and premises. Employees are required to take extra care that no websites or emails with suspicious content are being opened/downloaded on the Nursery School computers.*

Hopes and Dreams respects all employees' rights to a private life. However, Hopes and Dreams must also ensure that confidentiality and its reputation are protected at all times. We have therefore applied restrictions of access to websites, which include social networking, chat, gambling, and other sites that we consider to be inappropriate in the workplace. Employees must not post anything onto social networking sites, such as Facebook, that could be construed to have any impact on the Nursery School's reputation. Employees must not post anything onto social networking sites that would offend any other member of staff or parents. If employees choose to allow parents to view their pages on social networking sites then this relationship must remain professional at all times. Facebook and all social networking sites should not be used, accessed, or set up to follow a child's/young person's/parent's/carer's movements or activities. Do not monitor or investigate their social networking sites. If you come across their social networking accounts or sites do not enter them. This is uninvited intrusion into a family's life and you and your employer are liable to investigation if you act outside these guidelines. If you have any safeguarding/child protection concerns about a child's/young person's behaviour online, or if you think social media could provide critical information, for example, if a child is missing or is at risk of harm, the police and children's social care must be contacted. If warranted, the only agency that can access these sites is the police.

Cyber Bullying
Cyber bullying in any form will be regarded as gross misconduct and will lead to disciplinary action. If you feel that you have been subject to cyber bullying, directly or indirectly, by anyone connected to our organisation you should report this to the Nursery School Management immediately.

Printing Personal Items on Hopes and Dreams Printer/s and/or Photocopier
Please refrain from printing personal items on Hopes and Dreams' equipment. If the need arises to print personal items, as a matter of urgency, always obtain permission from the management prior to doing so. Company headed paper must never be used for printing purposes or for any other personal reasons.

Data Protection
When using any of Hopes and Dreams' systems, employees must adhere to the requirements of the *Data Protection Act, 1998*.

Remote Access
Employees who have remote access to Hopes and Dreams' emails and documents must strictly follow our Confidentiality Policy and the *Data Protection Act, 1998*.

Copyright Infringement
Employees must take care to ensure that they do not breach copyright or incur expense to Hopes and Dreams when copying, downloading, or sending material to third parties, however received or from whichever source.

Downloading or Installing Software
Employees may not install any software that has not been approved by the IT team onto Hopes and Dreams' computers or systems. Such action may lead to disciplinary action, up to and including summary dismissal in serious cases.

Using Removable Devices
Storing work related files on any removable drives (flash drives, external hard drives etc.) and/or taking company data outside of Hopes and Dreams' premises is not permitted at any time.

Monitoring of Communications

Hopes and Dreams reserves the right to intercept and monitor communications, including email, Internet use, and telephone calls. This also includes any mobile phone calls made on Hopes and Dreams' provided phones. If it is deemed necessary to monitor electronic communications, Hopes and Dreams will follow guidelines laid down by the Information Commissioner's Office to ensure adherence with the *Data Protection Act, 1998*, and any other relevant legislation.

Reviewed on: September 2019

Signed in behalf of the Nursery School:……

Next review date: September 2020