WALTHAMSTOW MONTESSORI SCHOOL

Policy on acceptable use of Computers, Mobile Phones and Cameras

At WMS we provide an environment in which children, parents/carers and staff are safe from inappropriate usage of mobile phones, cameras, IT equipment and the internet. A clear policy on acceptable use of these documents and facilities ensures the safety and wellbeing of children and their families and complies with the Data Protection Act 1998 and GDPR 2018, but also ensure staff, volunteers and students are not being distracted from their work with children. The policy must be understood and adhered to, without exception, by all parents/carers, staff and anyone with access to such devices or facilities whilst on our premises.

Mobile Phones

1. The school allows staff, volunteers and students to bring in personal mobile telephones and devices for their own use.

2. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

3. All Staff, volunteers and students must ensure that their mobile telephones/devices are left inside their bag throughout contact time with children. Staff, volunteers and student bags should be placed in a cupboard or locker.

4. Mobile phone calls may only be taken at staff, volunteers and student breaks or in staff, volunteers and student members' own time.

5. If staff, volunteers and students have a personal emergency they are free to use the school phone or make a personal call from their mobile in the office or Partridge Room only.

6. If any staff, volunteer or student has a family emergency or similar and requires to keep their mobile phone to hand, prior permission must be sought from the Principal and the mobile phone should be placed in the office.

7. Staff, volunteers and students must ensure that the Principal has up to date contact information and that staff, volunteers and students make their families, children's schools etc. aware of emergency work telephone numbers. This is the responsibility of the individual staff, volunteers and students.

8. All parent/carer helpers/students will be requested to place their bag containing their phone in a locker or cupboard in the office or another appropriate location and asked to take or receive any calls during breaks or when they leave the pre-school premises.

9. During group outings, nominated staff, volunteers and students will have access to a nominated mobile phone agreed by the school, which is to be used for emergency purposes only.

10. It is the responsibility of all members of staff, volunteers and students to be vigilant and report any concerns regarding the use of mobile phones to the Principal. Concerns will be taken seriously, logged and investigated appropriately (see allegations against a member of Staff, volunteers and student policy).

11. The Principal reserves the right to check the image contents of a member of staff, volunteers and students mobile phone should there be any cause for concern over the appropriate use of it.

12. Should inappropriate material be found then our Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures for the Staff, volunteers and student member's dismissal.

Cameras

Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form or recording their progression in the Early Years Foundation Stage. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.

1. Only the designated school cameras are to be used to take any photo within the setting or on outings.

2. Images taken on this camera must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
3. All Staff, volunteers and students are responsible for the location of the camera; this should be placed within the locked office cupboard when not in use.
4. The camera must be locked away at the end of every session.
5. Images taken and stored on the camera must be downloaded as soon as possible, ideally once a week.
6. Images must only be down-loaded by the nominated senior member of staff.
7. If the technology is available images should be downloaded on-site. Should this facilitiy not be available these may be downloaded off-site and erased from the personal computer as soon as the images have successfully been printed.
8. Photographs should then be distributed to members of staff, volunteers and students to record in children's learning journeys.
9. Under no circumstances must cameras of any kind be taken into the bathroom areas without prior consultation with the Principal.
10. If photographs need to be taken in a bathroom, i.e. photographs of the children washing their hands, then the Head of School must be asked first and Staff, volunteers and student be supervised whilst carrying out this kind of activity. At all times the camera must be placed in a prominent place where it can be seen.
11. Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

Computers

1. Information contained on the school computers should be identified as confidential or not confidential. Examples of confidential information include but are not limited to: company information and plans, competitor-sensitive information, users lists, and research data. Staff, volunteers and students should take all necessary steps to prevent unauthorized access to this information.

2. All PCs, laptops and workstations should be secured with a password-protected screensaver. Passwords are to be kept secure and accounts must not be shared. Authorized users are responsible for the security of their passwords and accounts.

3. Postings by staff, volunteers and students from the school email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own.

4. Staff, volunteers and students must not open any e-mail attachments received from unknown senders as these may contain viruses, spam e-mail, or Trojan horse codes.

Unacceptable Use

Under no circumstances are any staff, volunteers or students of the school authorized to engage in any activity that is illegal under local, national or international law while utilizing school-owned resources.

The following activities are strictly prohibited, with no exceptions. The lists below is by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the school.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the school or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a computing asset owned by the school to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any school account.

8. Effecting security breaches or disruptions of network communication.

9. Circumventing user authentication or security of any host, network or account.

10. Providing information about, or lists of, pre-school staff, volunteers and students to external organisation/s.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within WMS' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by WMS or connected via WMS' network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

(A signed policy is available upon request)

This policy was adopted on dated:1st March 2016

Date Reviewed: 01-09-2024
To be reviewed: 01-09-2025