Mayesbrook Park School

Alternative Provision for young people in Barking and Dagenham

E-SAFETY POLICY

JANUARY 2017

E-SAFETY POLICY

Version:	**2**
Approving Committee:	**The Governing Body**
Date Ratified:	**January 2017**
Reference Number	**2**
Name/Department of Originator/Author:	**Suresh Singh Mathusser Iqbal**
Name/Title of Responsible Committee/Individual:	**Annie Blackmore Head of MPS Chair: Robert Turner**
Date Issued:	**January 2017**
Review Date:	**January 2018**
Target Audience:	**Staff/Parents/Governors/LA**

Version	Date	Control Reason
Version 2	26/01/2017	Update

E-Safety Policy
Mayesbrook Park School (MPS)

The Governing Body, Head of Service and Staff will ensure that the policy is implemented equally in all cases, without regard to ethnic origin, cultural differences, gender, disability or sexuality issues. They will ensure that students are listened to and that their concerns are appropriately addressed.

This policy also governs all remote (off site) access to the resources of MPS whether they are by Terminal Services (RDT), Citrix Gateway (Oracle Finance), RM Integris, SIMS or some other means.

The term network refers to the MPS computer network.

The terms Staff or User(s) in this Policy refers to any contracted employee of MPS, employees of the London Borough of Barking and Dagenham or any person seconded to work at MPS. I.T. Technical staff are also included in and bound by this policy. The term User(s) also includes all students of MPS and parents who are permitted access to relevant school data delivered to them via its implemented Management Information System (MIS).

Introduction

The MPS network and the Internet resources it delivers offer access to a vast amount of information for use in studies and offering great potential to support the curriculum.

The computers and associated digital technologies are provided and maintained for the benefit of all staff, students, parents and visitors who are encouraged to use and enjoy these resources, and ensure they remain available to all. They should only be used for school and professional purposes.

Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn and possibly further disciplinary action. Any criminal activity will be handled by the relevant authorities.

School Equipment

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not deface or remove labels, logos or any other asset tags from PC related equipment.
- Do not remove or relocate any item of equipment from its installed location without permission. (This includes mice, keyboards or any other removable device that is the property of MPS.)
- Do not eat or drink near computer equipment.

- The maintenance of all computer equipment including printers (Particularly the removing of paper jams and the replacing of ink supplies) is the responsibility of qualified members of staff. If an item of computer equipment or a printer needs attention and this cannot easily be resolved, this must be directed to the I.T. Technical support team through the accepted call logging system ASAP.

Security and Privacy

- Upon arriving at MPS you will be issued with your own personal user account and space for work/educational purposes only. Do not disclose your account details (username/ password) to others, or use accounts intended for the use of others without the permission of SLT and the knowledge of the Network Manager/Senior I.T Technician.
- Do not use the computers and school systems in a way that harasses harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings unless you have been authorised to do so by the
- Computer storage areas will be treated with due privacy. By nature of the job Technical Staff do possess the ability to enter into any user's personal documents area. However, Technical Staff are also bound by this Policy and recognise the potential disciplinary implications of their job. Technical Staff may occasionally need to access your personal user area to resolve a problem and will obtain verbal permission from you before doing so.
- Technical Staff use certain software programs for remote maintenance and diagnostic purposes. When such software is used to resolve a technical problem, the recipient will be informed before a connection is made.
- MPS does also sanction the random spot monitoring of all activities on the network by authorised personnel.
- Data protection law requires that any personal information (e.g. staff or pupil records) will be kept private and confidential, and will only be used for the purpose for which it was collected / created. You should only share information with external organisations when authorised by the Head Teacher or designated member of staff. Every reasonable step should be taken to avoid accidental disclosure of confidential information (for example, by keeping login/password(s) private).
- Security of the school data is the responsibility of the user into whose trust it is held.
- If you use Laptop or Remote/USB storage device to transfer confidential information to and from the school this must be secured. This can be done either by purchasing a device with an encryption program or one with password protection. Documents produced in Microsoft Office also have a password protect feature.
- You should NEVER give out any school account names and passwords to anyone unauthorised.
- Staff Users should NEVER allow students to use staff level or office admin user accounts.
- Passwords should be changed periodically and/or when a person believes the account concerned may be compromised.
- Other than Class/Lesson registration documents/data, confidential Pupil Management/ Integris / SIMS data should not be accessed/ displayed in a classroom.
- Staff Users should log out of MIS/Pupil Management when not being used.
- When accessing confidential school data from home either via email or the Internet, care must be made to ensure that this is not seen by any unauthorised person.

- If Staff require information to be stored on a computer/laptop used at home, this must be first agreed with the Head of Centre and the device or local account used must be password protected and not accessible to other members of the household.
- Printing of any confidential/sensitive data whether at school or home must be treated as above. Discarded print jobs must be disposed of by shredding.
- Personal digital cameras or camera phones should not be used for transferring images of students or staff. Images will only be taken in accordance with MPS's Policy.
- Where negligence is found with regards to the above, disciplinary action may apply.

USB Storage/Cloud Storage (Off Site Data Storage)

- MPS has invested in and developed the computer network for the purpose of delivering educational/work resources and providing adequate secure data storage for all users. While there are clear advantages to storing information on USB Sticks, USB Hard Drives and storing data utilising Cloud Storage (e.g. Dropbox, ICloud and SkyDrive) please be aware that should the data also not be stored/ backed up first on the computer network that MPS will not be held responsible for any loss or corruption of such data.
- Since it is not possible for ICT Technical Staff to manage and administer personal cloud storage accounts they will not install on any school computer any client for off-site/cloud storage.
- Teaching Staff and School Admin Staff should not remove from the School Computer Network and store elsewhere any data that is deemed to be sensitive or potentially damaging to the School without first obtaining permission from the School.

Internet

- Do not access anything on the Internet that may be considered inappropriate for a work/educational environment.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Cyber Bullying or evidence of harassment will be dealt with in accordance with MPS's Anti Bullying/Disciplinary Policy and any Internet evidence collected may depending on circumstance be forwarded to the relevant authorities as part of an investigation.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws. Infringements of Copyright and Plagiarism will be dealt with in accordance with the relevant School Policies.
- You should not engage in any online activity that may compromise your professional responsibilities.
- School systems hold a full web history for all users of the network. MPS does sanction the monitoring of users Internet activity including the audit of Web logs/Web History by authorised personnel.

E-mail

- All staff users are automatically provided with a school email account. Selected student groups may be granted this facility. In most cases this E-mail account will also be available to access via the Internet off site/from home and is the responsibility of the user. This account must be used for all work related correspondence. **You must not use your personal e-mail account for any work related correspondence**. You may use your MPS E-mail for suitable personal correspondence as long as it does not contravene this Policy.

- Students are not generally permitted access to Personal E-mail
- Staff Access to Personal E-mail will be permitted but only via the Internet, for personal use and not to be accessed whilst supervising or in the vicinity of Students. You should never send confidential school data or professional information for the attention of other educational or Social Services via your personal E-mail. The same applies to information regarding the professional development or activities of fellow members of staff. Official School Information sent to parents should never be sent through a personal E-mail account.
- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Cyber Bullying or evidence of harassment will be dealt with in accordance with the MPS's Anti Bullying/Disciplinary Policy and any E-mail evidence collected may depending on circumstance be forwarded to the relevant authorities as part of an investigation.
- Never open attachments to e-mails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of e-mail containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist or inappropriate content. Always report such messages to a member of SLT.
- The receiving of unsolicited e-mail (Including spam) should be reported immediately to the Head of Centre. **Unsolicited e-mail however should never be forwarded to anyone, including technical staff in case it contains a virus**. An attached screen shot of the offending E-mail along with any relevant details will suffice.
- It is against data protection law to read the email or correspondence of another person without their expressed permission. Always check e-mail headers to make sure that the correspondence has been sent to you.
- E-mail correspondence will generally be treated with due privacy and in accordance with the law. The e-mail system nevertheless is the property of MPS. To this end the service does sanction the monitoring of e-mail traffic by authorised personnel, if it is believed that it is being abused.
- It is important that you are informed that all E-mail regardless of the network provider is subject to being swept for viruses and other content that may contravene the law. Occasionally email sent into or from the school may be trapped because the system put in place to monitor this (managed away from the School) believes that it meets a certain criteria. It is remotely possible at this stage that a public official or third party engineer may have to view the contents of an E-mail to assess the reason for the system trapping it.
- Remote access to School E-mail should be via the agreed system for web access. POP 3 access is currently permitted to Staff for access on a mobile device where permission has been obtained and an agreement to abide by school Policy has been signed. It should be recognised that there is an increased potential for Confidential School Data to fall into the wrong hands and therefore it is stipulated that:
- The device is set to keep only a maximum of 3 days mail at any given time and that the settings are not adjusted.
- These mobile devices should not be devices shared with other persons/family members who are not affiliated with MPS.

- Although these mobile devices are your personal property, MPS e-mail system is not, and therefore you have a responsibility to inform MPS if the device has been compromised, lost or stolen.
- If the Mobile Device has a password protect feature this should be enabled.
- Failure to adhere to this advice could result in disciplinary action.
- Personal e-mail is defined as an e-mail account that you set up with another network provider. Examples of personal e-mail include Hotmail, AOL, BT/Yahoo, and Gmail. While every attempt is made to ensure that you have access to the mail websites, this is Internet dependent and also subject to filtering.

Network Monitoring

The Network/Communication facilities are the property of MPS, and because a potential exists for abuse, MPS reserves the right to authorise personnel, in accordance with what is legally acceptable, to embark on any investigative process that involves the monitoring of a person's user space or E-mail communications. If any breach of school policy breaks the law, disciplinary action will follow and any evidence produced may be retained for and passed over by authorised persons to relevant authorities in accordance with the law and data protection legislation.

Personal Activities

The MPS school network and associated Digital Technologies have been provided for the purpose of delivering the school curriculum and resources that are appropriate for a secondary school environment. Personal interests and activities such as booking holidays and flights, buying or selling should only be done in an emergency. School email and telephone systems should be used for school business only.

Social Networking

- Social networking sites however popular are not permitted whilst at school.
- It is accepted that staff in certain Job roles (particularly Pastoral and Child Protection) may at times need to investigate certain cyber abuses on Social networking sites. Permission to access Social Networking Sites may be granted for this purpose only. Application must be put in writing to the Head of Centre (or an agreed representative).
- It is not advisable for members of Staff to befriend students who are not family members on Social Networking Sites.
- Although MPS does not legislate over the use of these sites away from school/work it is important to note that any material published on social networking sites regarding the personal or professional activities of students.
- . If a fellow member of staff or any other Public Official of the London Borough of Barking and Dagenham asks you to remove content from a Social Networking site, you should comply.
- Images of School sponsored events should not be posted on social networking sites, especially if these contain photographs of students or persons affiliated with MPS, unless expressed permission has been given by the MPS.
- MPS will assume the responsibility to discipline any user who fails to comply with the above.

Child Protection Issues

- Child abuse images (or potential child abuse Iimages): A child abuse Image, or "Indecent Image of a Child" is an image of a sexual nature that depicts a child under the age of 18. **Any printing, e-mailing, or copying of a child abuse image is an offence under uk law.**
- If while in a working capacity you come across images of this nature DO NOT do anything until you have discussed the matter with the relevant Designated Safeguarding Lead (DSL). If displayed on a student's computer screen remove the student(s) and seek immediate advice. **Do not show any child (any person under 18) the image even if to ascertain for example the source or culprit of a printed or sent image**.

- Adult Pornography: **an offence against uk law may be committed if an adult pornography image is shown to a child even if to ascertain for example the source or culprit of a printed or sent image**. Again DO NOT do anything until you have discussed the matter with the relevant DSL first.

- Relevant Child Protection Personnel should carry out all investigations of the above and should be the person(s) who through consultation involve ICT Technical Personnel where appropriate.

MPS Loaned Computer Equipment:

- Any computer or laptop loaned by MPS, is provided solely to support staff professional responsibilities and that the centres should be notified of any 'significant personal use' that would deem the device a benefit as defined by HM Revenue & Customs.
- All loaned equipment should not leave the confines of the centre, unless it has first been security marked and added to the School Equipment Asset Register.

This policy should be read in conjunction with our Safeguarding Policy.