ROBERT CLACK COMPUTER RESOURCES AND E-SAFETY\ACCEPTABLE USE POLICY (AUP)

This Computer Resources policy governs all access to the Systems and Digital Resources of the Robert Clack School, whether they be "Networked" or "Standalone", accessed internally or externally via a Web Browser, via the Designated School "RC" Wireless Network, Remote Desktop- *Terminal Services*, *or* by some other means. This Policy covers all authorised access to School data hosted on third Party Systems such as the *SIMS.Net*, *The SIMS Learning Gateway* (SLG), the School's Registered *Google Apps/Google Classroom* Domains and *RM Finance.*

The terms *The School, Robert Clack School or Robert Clack School of Science* refers to all facilities and systems considered to be under the jurisdiction of the said school or secured by the said school for educational means and includes the use of the *Robert Clack School computer* network, *Microsoft Exchange Email*, the *School's Learning Gateway site, Google Classroom, Google Applications* and the *Robert Clack Leisure Centre* ICT facilities.

The term *Network* refers to the Robert Clack School computer network, the Registered School Domains *"robertclack" "robertclack.internal, robert-clack.bardaglea.org.uk, robertclack.co.uk* **and all Google Domains that are registered and owned by the School for Educational and professional Use.**

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

This Acceptable Use Policy incorporates the School Best Practice and E-Safety policies.

Introduction

The School has provided an array of Computer Related Equipment and Digital Technologies for Educational use and Student support. It has also invested considerably in developing its network infrastructure. The School 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

Software programs and applications should not be installed without first seeking advice and permission from those persons held responsible for managing the school ICT Equipment.

School Computer Equipment and related Digital Technologies should be treated in accordance with the instructions for use and the purpose it was made. Anyone found to be damaging or defacing any aspect of the School equipment will be reported to SLT.

Labels, logos or any other asset tags placed on Computer related equipment should not be removed unless authorised.

School Computer Equipment should not be moved or relocated without permission. (This includes mice, keyboards or any other removable device that is the property of the said school.)

You are permitted to bring your own Data Storage Devices (USB Memory Sticks/ Flash drives) and Storage Media into school for *work/educational purposes only*. The School will not be liable for the theft, loss or damage of these devices/media.

If you suspect that your device/media may contain a virus, DO NOT CONNECT OR LOAD IT INTO ANY COMPUTER EQUIPMENT WITHIN THE SCHOOL WITHOUT FIRST CONSULTING TECHNICAL STAFF. Users are responsible to ensure that these devices/media are checked by reputable antivirus software before bringing them into school.

You should not connect mobile related devices to the network (e.g. laptops, tablet PCs, Smart Devices, IPods, MP3/4 players, Mobile Phones, etc.) without first checking that this is permissible.

Eating or drinking near classroom computer equipment is not advised.

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 Robert Clack School you will be issued with your own personal user account and work 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 permission of the owner or the School.

Do not use the computers and school systems in a way that harasses, harms, offends or insults others. Anyone found to be inciting hatred, engaging in illegal activity or conducting themselves in any way out side of the ethos of the School shall be reported to the relevant authorities.

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.

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 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. *The School does also sanction the random spot monitoring of all activities on the network by authorised personnel**.

The School sanctions the use of interactive classroom teaching tools with remote monitoring capabilities. These tools require that a software client is installed on the computers and laptops. This software must be used responsibly and in accordance with School Policy.

- The School employs various systems that monitor potential network abuses, such as the use of foul, offensive and obscene language. These systems run in stealth on every network computer and laptop. When a violation takes place a copy of the violation is held on a secure computer system. These tools are generally used for investigative purposes *although the School does sanction the use of these systems for random spot monitoring of all activities on the network by authorised personnel*.*

**For more Information, please see the section on Network Monitoring*

School Password Policy

All users of the School Network should take seriously the importance of maintaining a secure and safe working environment. To this end all Staff Users are supplied with a set of secure login details that provides them access to both personal and communal areas of the Network.

The username and password governs which areas of the School Network a User will be permitted access to. This single username and password also provides a User with access to a personal Mail Box (*Microsoft Exchange*) and the *SIMS.net* Client (The *SIMS Learning Gateway* or *SLG* however requires a completely separate set of user credentials for accessing SIMS.net over the Internet). With this in mind please note the following:

- that it is a breach of School Security and Data Protection Policy to allow any Student or Non-Authorised person access to your School Network Account by giving them your secure password and or by allowing them to log on to the network as yourself. If you believe your School Network Account to be compromised this way you must change your password immediately and notify your Line Manager.
- All Staff User and Administrative Passwords will be reset at the beginning of every Term. Staff Users will be given adequate notice of the change. Once the change is enforced by the Network Administrator you will be asked to change your password at the next login.
- It will not be possible to access the School Network including your Mailbox remotely\away from School (Via the Outlook Web App or Smartphone) once a password change has been enforced by the Network Administrator. You will first need to change your password in School to gain access to these features again. If you will be away from school for a prolonged period, you will need to contact the Network Administrator and make special arrangements for renewed access.

Security of School Data

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.

The School Pupil Management system (Currently SIMS.net and The SIMS Leaning Gateway) is instantly accessible to Authorised Teacher and Non-Teacher Users of the Robert Clack School Network via their designated User Accounts and Secure Passwords. Please note that it is a breach of School Security and Data Protection Policy to allow any Student or Non-Authorised person access to your School Network Account by giving them your secure password and or by allowing them to log on to the network

as yourself. If you believe your School Network Account to be compromised this way then you must change your password immediately.

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.

Departments should not share accounts. Generic accounts (Accounts set up for multiple users or a department) will not be permitted unless agreed by SLT.

Other than Class/Lesson registration documents/data, confidential Pupil Management/ SIMS.net data should not be accessed and displayed in a classroom.

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 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 pupils or staff. Images will only be taken in accordance with the School's Policy

Where negligence is found with regards to the above, disciplinary action may apply.

School Wireless Network

Staff users are permitted to use the School Wireless Network where this is available and once connected are bound by this policy regardless of whether the device is a School Owned or Personal Device. Staff users access the wireless with their School User Credentials. STUDENTS ARE NOT CURRENTLY PERMITTED ACCESS.

You should not give out your username and password out to anyone especially students as this will be considered a breach of School Policy and your access will be revoked.

There is a guest facility for Official School Visitors who have Registered via the Sign in System. It will be in the form of a username and password that will be changed regularly and emailed to Reception Staff and the Head's Personal Assistant.

USB Storage/Cloud Storage (Off Site Data Storage)

The School has invested in and developed local Network Systems for the purpose of delivering Educational/Work resources and providing adequate secure data storage for all users. The School has also a registered Google Classroom Domain that is used for teaching and learning.

While there are clear advantages to storing information on USB Sticks, USB Hard Drives and storing data utilising Cloud Storage solutions please be aware that should the data also not be stored/ backed up FIRST on Domains and Systems owned or registered

for use by the School for teaching and learning, that the School will not be held responsible for any loss or corruption of such data.

ICT Technical Staff will not be permitted to install on any School Computer any client for off-site/cloud storage that the School is not responsible for.

Teaching Staff are responsible to make it clear to their students that USB Sticks and Cloud Storage Solutions should be only used **as a backup** for work already existing on the School.

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\Internet Filtering

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 the School'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.

The School has systems in place that filter monitor Internet activity and filter unsuitable websites. This is done as a legal requirement and for the protection of young persons. The School decides which websites should be filtered.

It is illegal to use the internet to obtain and use information that enables a person to bypass the security features put into place for the purpose of protecting young persons. Anyone found to be actively accessing websites normally prohibited will be reported to SLT.

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. *The School does sanction the monitoring of users Internet activity including the audit of Web logs/Web History by authorised personnel.*

E-mail

Users are automatically provided with a school email account. 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 School related correspondence**.

STAFF USERS MUST NOT USE THEIR PERSONAL E-MAIL^ ACCOUNT FOR ANY WORK RELATED CORRESPONDENCE. They may however use their Robert Clack E-mail for suitable personal correspondence as long as it does not contravene this Policy.

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 School'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 I.T. Technical support team. Where such unsolicited E-mail is of a violent, dangerous, racist or sexually explicit nature, SLT should also be informed. 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 the Robert Clack School. *To this end the School does sanction the monitoring of E-mail traffic by authorised personnel, if it is believed that it is being abused.*

Remote access to School E-mail should be via the agreed system for web access. Access is currently permitted to Staff on a personal mobile device\smartphone\tablet 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 Robert Clack School.
- Although these mobile devices are your personal property, the ***Robert Clack School E-mail system is not***, and therefore you have a responsibility to inform The School 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 the Robert Clack School, and because a potential exists for abuse*, the School 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 Robert Clack 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.

- Although there is some flexibility allowed for personal use of the Internet whilst in work (e.g. lunch breaks) you should not be found to be using these resources for personal use or gain at times when you are supposed to be Teaching, Working or "On Duty".
- You should not be found to be using the Internet to access information or resources that are considered Inappropriate for an educational environment.
- User Internet history is recorded and this may be used as evidence where it is believed that there has been flagrant abuse of Internet privileges.

Social Networking

Social networking sites however popular are not permitted whilst at school.

It is however 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 (or an agreed representative). If granted the Network Manager will be instructed to make the policy change.

It is not advisable for members of Staff to befriend Students who are not family members on Social Networking Sites.

Although The School 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, fellow members of staff or any other Public Official of the London Borough of Barking and Dagenham should not be found to be defamatory or offensive.

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 the School, *unless expressed permission has been given by the School.*

The School 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 Images): 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 Child Protection Personnel. 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 Child Protection Personnel 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.

School Loaned Computer Equipment

Any computer or laptop loaned by the school, is provided solely to support staff professional responsibilities and that the school 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 school unless it has first been security marked and added to the School Equipment Asset Register.

Approved by the Governing Body of Robert Clack School Updated 20/02/17