Osmani Primary School
Vallance Road
London
E1 5AD

Tel: 020 7247 8909
Fax: 020 7247 9906
Email: admin@osmani.towerhamlets.sch.uk

www.osmani.towerhamlets.sch.uk

Osmani Primary School

Reach For The Stars

ICT Security and Staff Acceptable Use Policy

Our Motto

Reach For The Stars

Our Vision Statement

Our vision is to develop an inclusive school, which promotes and achieves excellence, and continues to nurture the values, confidence and skills of pupils, staff and the community, in order to meet the emerging opportunities of the 21st century.

Our vision and values support **Articles 2, 12, 15, 19, 24, 27, 28, 29, 31** of the UN Convention on the Rights of a Child.

Our Rights

- ★ **Article 19:** We have the right to be safe.
- ★ **Article 28:**We have the right to quality education.
- ★ **Article 12:**We have the right to give our opinion and listen to others.
- ★ **Article 15/31:**We have the right to join in and be part of a team.
- ★ **Article 29:**We have the right to develop our personalities, talents and abilities.

Our Values

Striving Teamwork All Included Responsibility Success

★ Striving

Our aim is that we are a school that:

- **uses our Growth Mind-set (learning from mistakes and always willing to have a go)**
- **never gives up and always find ways of improving**
- **enjoys challenges and aims high**

★ Teamwork

Our aim is that we are a school that:

- **encourages and supports each other to be the best we can be**
- **learns from each other**
- **listens to and respects each other's ideas**

★ All Included

Our aim is that we are a school that:

- **has high expectations of everyone**
- **encourages everyone to take an active part in learning and life of our school**
- **nurtures and celebrates what makes each and every one of us unique**

★ Responsibility

Our aim is that we are a school that:

- **takes ownership of the choices we make**
- **takes ownership/charge of our own learning**
- **looks after each other and our school**

★ Success

Our aim is that we are a school that:

- **provides an education that encompasses academic, creative, social, emotional, physical and cultural development.**
- **celebrates our efforts and achievements**

Equal Opportunities and the Single Equality Scheme

We believe that all those who work in Osmani - children and adults - have the right to be treated fairly and with respect by everyone connected with the school.
We aim for Osmani to be a safe, supportive place, where all children and adults feel valued as individuals, whatever their ability, age, disability, gender identity, marriage or civil partnership, pregnancy & maternity, race, religion or belief, sex and sexual orientation.
The school aims to foster the social and personal skills of co-operation, sharing and mutual respect.

This policy supports the school in addressing Article/s 29: of the UN Convention on the Rights of the Child.

Introduction

Osmani Primary School is committed to preserving the confidentiality, integrity and availability of all the electronic information assets throughout the school. This is critical to the on-going functioning and good governance of the school.

Information Communication Technology (ICT)

Information Communication Technologies encompass a range of devices, platforms and systems that store, process and share information and data. They can include:

- Computers and laptops
- Server-based networks
- Mobile devices (tablets, phones etc)
- CCTV Cameras
- Removable storage devices
- Digital cameras
- Sound recording devices
- Learning platforms/digital library resources
- Cloud-based platforms and networks
- Cloud-based applications and tools

This ICT Security Policy outlines the school's approach to electronic information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the school's electronic information systems. The school is committed to a robust implementation of ICT Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its electronic data. The principles defined in this policy will be applied to all of the electronic information assets for which the school is responsible.

Roles and Responsibilities

ICT Security is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

Senior Leadership Team (SLT)

The SLT ensures that the policy is implemented and compliance with the Policy is monitored.

ICT Security Manager

Our school ICT Security Manager is Levett Consultancy.
They keep up to date with Information Security issues and guidance and ensures the SLT are updated

Governors

The Governing Body has a responsibility to ensure that the ICT Security Policy is updated and monitored regularly. We ensure our governors are aware of local and national guidance on ICT Security and are updated regularly.

School Staff

All school staff are required to understand the policies relating to ICT Security, and the rules and restrictions that are part of the agreement that they sign each year

Parents

The Information Security policy is available to parents on the school website, and a printed copy can be requested

Other Related Policies

The ICT Security Policy forms part of a suite of policies addressing the range of data protection and online safety issues that schools must address. These include:

- Data Protection and GDPR Policy
- Pupil Online Safety Policy
- ICT and Computing Curriculum Policy

Internet Access

School Internet Provision

The school uses Virgin Media Business, as part of the London Grid for Learning (LGfL) Broadband consortium. Virgin provides an always-on broadband connection at speeds up to 100 MB.

Internet Content Filter

The LGfL use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined in the Pupil Online Safety Policy

Classroom and User Management

The school uses **Impero**, a network management and monitoring tool that reports any misuse or violation of the school's filtering strategy by any user (staff and pupils) to the ICT Security Manager

- Key words will trigger a report, and categories include Terrorism, Bullying, Gambling etc.
- The report is sent directly to the Headteacher and ICT Security Manager/Lead ICT Technician
- Issues arising from this monitoring will be reported to the relevant SLT/Safeguarding staff member

Downloading Files and Applications

Pupils and staff should not download/install any material from the Internet onto any school device or system.

Security and virus protection

The school subscribes to the LA/LGfL Antivirus software program, which uses Sophos and Norton Antivirus software. The software is monitored and updated regularly by the school technical support staff.
Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the Technical Support Service and/or ICT Security Manager

Connection of personal staff devices/external agency devices to the Internet

On occasion a staff member or an external party (eg School Nurse) will need to connect an external device to the school Internet service. The school has a secure guest Internet access account for this purpose. Access information is available from the school office.
This Internet access can be monitored and should only be used for professional purposes unless agreed with SLT.

The School Network

The school has a server-based network with staff-only and shared drives. Staff are given access according to the school's ICT Access Control guidelines – see below.
The server is accessed through laptops and computer workstations in classrooms, offices and meeting rooms around the school. Staff have access to relevant drives according to their role and responsibilities.
Only authorised Technical Support Services staff have access to the server itself and are able to change settings and profiles etc.

Google Education

All Pupil and Staff Drives are now online within the school's **Google Education** installation rather than on the physical server as the school moves towards a cloud-based system.
Staff are set up with Google accounts that give appropriate access to the various Google drives and tools

Other Cloud Based Services

The school subscribes to several approved cloud-based services that provide tools, storage and applications for both staff and pupil use. These accounts include:

- A school authorised Google Education account which gives access to the school Google Platform
- A Purple Mash Staff account which gives access to the school Purple Mash Learning Tools suite
- And other authorized accounts

ICT Access Control

Access to school ICT systems for new staff users is authorised by SLT and then provided by the authorised Technical Support Services. Network settings ensure that passwords are suitably complex and are updated regularly in line with best practice and the GDPR.

Access management

A database of staff users, their access rights and credentials is kept securely in line with GDP Regulations by the Technical Support Officer and can be reviewed when necessary by SLT.
Staff access is automatically terminated when they leave the employment of the school.

The following accounts are provided:

- A school network username and password for access to the school server network
- A school Google Education account
- An LGfL Unique Sign On (USO) account which acts as their official staff email account (via LGfL StaffMail) and also gives access to LGfL resources and tools

Cloud-based tools and platforms

Staff accounts for these services are controlled in the same way as other access to ICT services

Restricted Access

Some users are granted access to restricted areas of the network or cloud-based storage on the basis of their roles and responsibilities as agreed with SLT. These credentials must be kept private and secure and not shared with other staff members.

Remote Access

The school provides access to some areas of the school network remotely. This allows staff to log in to the school network from outside school to retrieve documents and files. Files may be downloaded for editing and then re-uploaded to the school server.
Staff may also access cloud-based storage and information systems outside school.

Any school files containing personal information downloaded to personal computers, tablets, phones or tablets for editing should be deleted from these devices immediately in line with the GDP Regulations and Data Protection Policy.

Remote access to school systems is restricted to those specified staff who need access and removed immediately when a staff member leaves the school.

Visitors

All visitors (including supply staff and contractors) to the school will be made aware of the general safeguarding arrangements of the school on arrival, and the key elements of the staff ICT Security Agreement as it relates to their visit.

- Access to the school network and Internet services on any device will not be given unless set up and supervised by an appropriate school staff member who has full knowledge of the ICT Security Policy.
- Visitors will not have access to online devices unless agreed by the Senior Leadership Team, and for a defined purpose related to their visit. (eg the school nurse may need to access the guest Wi-Fi password to allow access to materials and resources relevant to the visit)
- Visitors will not be permitted to take any photos or make digital video or sound recordings of school activities or resources unless specifically agreed beforehand with the Senior Management Team.
- Visitors agree to abide by professional standards in the dealings with the school, and to maintain these standards outside school once the visit has ended. This includes social media and other online platforms
- Visitors agree that personal mobile phones and other digital devices must be kept out of sight and switched to silent mode in the presence of pupils and parents

Supply/Temporary teaching staff

Short Term Supply staff will not be given their own access to the Internet and network. They will be given access by a generic **supply staff user account** that has restricted access to the school network.
Documents stored in the My Documents area of this account will be deleted and the password changed regularly
Access to other systems and cloud-based services will be given on an individual basis as the need arises, according to the discretion of the ICT Security Manager/Senior Management Team.
Supply staff will be given a printed summary of this policy as part of the **Supply Teacher and Visitor Information Sheet** and asked to sign the **Supply Staff ICT Security Agreement** when they arrive at school.

School Mobile Devices

School staff may use a selection of mobile ICT devices to support teaching and learning and to ensure the safety of pupils and staff. They may be used in school and outside school when authorized by SLT.
These currently include:

- **School mobile phones** – used on school trips to communicate securely with school
- **School tablets**

All of these devices are managed by the school and have appropriate restrictions and security features enabled. They are regularly checked and updated by the Technical Support Services. Use of these devices is monitored by the ICT Security Manager and they are signed in and out by staff via the school office administrator
They are not used in any circumstances for staff personal business.

Disposal of ICT Equipment with data storage

All school equipment that may contain information or data will be disposed of using an approved Third-Party Company that will provide a certificate of disposal. **See the GDPR Policy for more information.**

Use of the Internet and ICT resources by school staff

Professional use

- Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils
- Staff also consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.
- Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the ICT Co-ordinator.

Personal use of the Internet and ICT resources

- We recognise that staff may occasionally find it useful to use the Internet at work for personal purposes
- However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the staff agreement form below

Personal devices in schools

Staff may bring in their own devices to school on occasion. They are not allowed to connect these devices to the school network without permission from the SLT and this connection must by initially set up by Technical Support Services if agreed.

Use of personal devices to capture digital media

The use of personal devices to capture or record digital images, sound or video is not permitted unless agreed beforehand with the ICT Security Manager and/or the Senior Management Team. If permission is given, then any images, sounds or videos should be deleted completely from the device once transferred to the school network or data storage.

Email accounts

- Staff members will be given a school e-mail address (which is also their LGfL USO account) and should use it for all professional communications
- Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

Online discussion groups, bulletin boards and forums, online chat and messaging

- The use of online discussion groups and forums **relating to professional practice and continuing professional development** is encouraged
- staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.
- The personal use of these services is strictly forbidden on school premises or on school equipment

Social Networking

- The school has a social media presence that is strictly monitored by the ICT Security Manager/SLT/designated staff member
- Staff wishing to contribute to school social media accounts should only do so with permission from SLT and using approved school devices
- The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements

Data Protection and Copyright

- The school has data protection policy in place – please see the **GDPR and Data Protection Policy** for more details.
- Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.
- Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

Staff Laptop and ICT Equipment Loans

Some equipment is available for loan to staff, with permission from the ICT Security Manager and Headteacher. The appropriate forms and agreements must be signed. Loaned equipment must only be used for professional purposes, both in and out of school.

- Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment or device must adhere to all aspects of this ICT Security Policy.
- This must be the case wherever the laptop, computer or other such device is being used as it remains the property of Osmani Primary School at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense

Use of ICT during school closures and for home learning

What the school is doing to providing appropriate and secure online learning tools/systems for staff

- Ensuring all platforms and online communication tools used to communicate with pupils are secure, appropriate and are part of a robust school managed system
- Liaising with technical support staff to ensure robust security for remote access to school network resources and online learning tools, including secure management of staff and pupil accounts/passwords
- Ensuring staff and pupils know the difference between material that is public (eg on the school website), shared with school pupils (a class blog) and private between a pupil and their teachers (a 2Do comment)
- Providing staff with support and INSET where needed to develop the skills to provide Online learning
- Disseminating up to date information from Government and other organisations to staff

What staff are doing to ensure the online learning they deliver is safe, appropriate and professional

- Only using systems provided or agreed by the school to communicate with pupils and families
- Remembering to be particularly careful about posting images of children with identifying information, especially if the photo was taken at the pupil's home.
- Ensuring that any devices logged in to school remote learning or cloud-based resources are supervised and logged off when not being used
- Ensuring that all pupil data and information stored on their personal devices (with permission from the school) is deleted as soon as it is no longer needed
- Ensuring they are up to date with all relevant school policies, and asking for clarification if needed

Safeguarding: Children and online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the schools Safeguarding and Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the teaching code of conduct, the ICT Security Policy and Staff Agreement, and the Pupil Online Safety Policy. East End Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Blogs and learning platforms will be monitored daily by SLT and any concerns will be addressed immediately. Online Safety Support and resources for parents and families will be clearly signposted on the school website. Parents and Children should be made aware of how to report online abuse through clear routes such as; UK Safer Internet Centre and CEOP

Staff understand that they should:

- only use online platforms and tools suggested by East End Primary School to communicate with pupils.
- only use school-registered accounts, never personal ones
- Avoid 1:1 communication unless pre-approved by SLT

Care should be taken to ensure that photos and videos made at home by staff and shared with pupils uphold professional standards. Below are some things to consider when delivering remote learning/lessons, especially where webcams or uploaded photos are involved:

- Staff and children must wear suitable clothing in photos or video links, as should anyone else in the household/background.
- Any computers or devices used by staff or pupils should be in appropriate areas, for example, not in bedrooms or bathrooms
- Care should be taken to ensure that any areas of private homes seen on video or in photos, (eg furniture, wall art and other personal items) are appropriate
- Language (including from anyone else in the household) must be professional and appropriate
- Background sounds must be minimised as much as possible

School Staff ICT Security Acceptable Use Agreement Form

This document covers the use of school digital technologies and networks in and out of school.
Some aspects of this agreement are also covered in other policies and contracts

Access

- I will not reveal my password(s) to anyone other than the appropriate staff managing the system
- If my password is compromised, I will change it immediately and inform the ICT Security Manager
- I will not use anyone else's password if they reveal it to me
- I will ensure that all passwords are updated when required and follow any rules for complexity etc
- I will not allow unauthorised individuals to access school ICT systems or resources using my access details

Remote access

- I will keep any login details for remote access (Purple Mash, Google Education etc) secure
- I will always log out completely from any device when my remote access session is finished
- I will never save passwords or login details on any device outside school
- I will take all reasonable precautions to ensure my remote access session is secure
- I will not download sensitive personal data onto any non-authorised device or system
- I will not allow any other person to access or edit any school account, website or other digital platform
- I will ensure that all pupil data (with permission) stored on personal devices is deleted when it is no longer needed

Appropriate Use

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to SLT

Email

- I will only use the approved, email system for any school business or communication with parents
- I will not communicate with pupils by email unless using approved school email accounts as part of schoolwork.

Professional Conduct

- I will not engage in **any online activity** that may compromise my professional responsibilities
- I will ensure that any private online content that I create orm contribute to are not confused with my professional role
- I will ensure that my activities on social media do not breach professional conduct standards
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when using ICT to communicate
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to/receipt of inappropriate materials, or filtering breach to the ICT Security Manager

Photographs and Video

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance).

Personal Use

- I understand that I may use ICT for personal use only where resources are not being used and no pupils are present
- I will not download any attachments, pictures or other material onto school computers, or onto any school network
- I will not use the school internet facilities or school devices to access personal social media accounts

Teaching and Learning

- I will always actively supervise/arrange for suitable supervision of pupils that I have directed to use the Internet.
- I will teach the school Online Safety curriculum using agreed resources and materials
- I will ensure I am aware of digital safety-guarding issues so they are embedded in my classroom practice.
- I will only use the Internet for professional purposes when pupils are present

Copyright

- I will not publish or distribute work that is protected by copyright.
- I will teach pupils to reference online resources when they use them in a report or publication.

REMOTE AND HOME LEARNING

When I am communicating with pupils and families I will:

- Only use systems/accounts provided by or agreed by the school to communicate with pupils and families
- Not conduct livestreaming lessons or video calls with pupils or families unless agreed beforehand with SLT
- Be conscious of safeguarding issues when communicating with children via using Gmail, Google Classroom, Purple Mash discussion forums or any other approved online communication platform
- Immediately contact the Designated Safeguard Lead if I have any concerns regarding safeguarding

When I am writing, creating and publishing content on the school website I will:

- Ensure that everything I publish online to support home learning is appropriate and suitable for children
- Check written materials that I create and post online for grammar and spelling mistakes
- Check thoroughly all external resources that I am recommending or linking to for suitability
- Consider SEND, accessibility and the needs of the intended audience when creating resources
- Avoid infringing copyright when copying books, resources and images and publishing them online

When I am creating any media content that will be published to the school website I will:

- Record media in a neutral area where nothing personal or inappropriate can be seen/heard in the background
- Dress appropriately and professionally and use appropriate language and vocabulary
- Ensure that any materials and media produced are of a suitable quality and standard before publishing
- Only use school video sharing accounts (Vimeo) to upload and embed staff-created videos on the school website.

When I am publishing content created by pupils and families I will:

- Ensure that I have the parent's permission to post images taken in the family home
- Clarify with parents the school policy on what kind of images and videos the school will can publish
- Carefully scrutinise images and videos before publishing to ensure school policy is being followed
- Check images of children for identifying information, especially if the photo was taken at the pupil's home.

Use of school equipment out of school

- I understand that any device loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will keep any 'loaned' equipment up-to-date and will return it when requested to be updated by a school technician.

Data protection

- I have read the school GDPR and Data Protection Policy
- I agree to abide by the rules set out in the GDPR and Data Protection Policy at all times
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

User Signature

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent ICT Security and Data Protection policies

Signature _____ Date _____

Full Name _____ Job title _____

Agreement for access provision

I approve this user to have access to the school network and Internet provision as outlined below:

School Network Account		SLT Access to restricted areas		Access to restricted SEND areas	
LGfL USO/Staff mail account		Purple Mash Staff Account		Espresso Staff Account	
Other:		Other:		Other:	

Authorised Signature (Head Teacher)

Signature _____ Date_____

Full Name _____(printed

Staff Laptop and ICT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment or device must adhere to all aspects of this ICT Security Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of East End Primary School at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement before taking the equipment away from the school premises.

Staff ICT Equipment Loan Agreement

I have borrowed a school ICT Device to use out of school in agreement with both Head Teacher and the ICT Security Manager.

Device Type	Make	Model	Serial Number	Date Loaned	Date Returned

It is understood that I will return the equipment to school if requested to do so by either the Head Teacher or the ICT Security Manager

- I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage.
- I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace or arrange for the repair of the equipment at my own expense.
- I will use the equipment in accordance with the school ICT Security Policy and GDPR and Data Protection Policy.

I agree to the above conditions:

Signature Date

Full Name (printed)