



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

★ **S**triving **T**eamwork **A**ll Included **R**esponsibility **S**uccess ★

★ 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

This 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
- Remote Learning Policy
- Staff Professional Conduct Policies and Guidelines
- Artificial Intelligence (AI) Policy

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 school's Internet filtering and monitoring system is provided by the **London Grid for Learning (LGfL)** and is managed for the school by **the School ICT Technician** who can liaise directly with the LGfL filtering team.

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.

Staff have been issued with clear guidelines on what to do if this happens.

Staff who deliberately try and access unsuitable materials will be dealt with according to the Staff Code of Conduct

Third Party Filtering

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 pupil) 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 ICT Security Manager/Lead ICT Technician
- Issues arising from this monitoring will be reported to the relevant SLT/Safeguarding staff member

The School Network

The school has a **cloud-based network using Google Education** platform.

- Document and file storage drives are cloud-based with staff-only and shared drives.
- Staff computers are set up to allow staff to interact with folders and files on the Google drives in the same way they did with the previous server-based network using yellow folders in File Explorer.
- Staff and pupils have their own Google accounts that are set up and administered according to the school's ICT Access Control guidelines – see below.
- When accessing the Google drives away from school, staff use the standard Google web-based interface.
- The Google Education platform is managed remotely by the school's ICT Technical Support Team – currently provided by Levett Consultancy.

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 Purple Mash Staff account which gives access to the school Purple Mash Learning Tools suite

Staff email

Google Mail

Staff email is provided using the Google education platform via individual staff Google accounts. This email address should be used 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.

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 and their access rights to the school Google network and any other cloud-based platforms and resources 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.

Restricted access

Some users are granted access to restricted areas of the network (eg SEND information) 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.

School Hardware and Devices

Computers and laptops and tablets

The school has a range of hardware devices that are part of the school network.

These include:

- Desktop computers
- Laptop Computers – Windows
- Chrome Book laptops
- Tablets – iPads
- Interactive Whiteboards
- LED Display screens

Non-computer-based devices

The school also provides a range of non-computer based digital devices for educational use.

These include:

- Digital Visualizer/document cameras
- Digital cameras
- Digital robots (BeeBots etc)
- Lego WeDo Kits
- School mobile phones

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.

Reporting faults and damage

Staff are expected to ensure these devices are used safely and appropriately by themselves and pupils. Any damage, faults or other technical problems should be reported to the ICT Technical Team (using the appropriate fault reporting system) and the ICTCO.

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

Visitors

All visitors (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. These elements include:

- 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 be given access to the school network and resources via a generic **supply staff user account** that has restricted access. Documents stored in the personal 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.

Professional use of school ICT and Internet resources

- 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.

School Social Media Accounts

- 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

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.

Use of Artificial Intelligence Tools

Approved use of AI

We are committed to helping staff and governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert. This means that we have the following rules in place for staff.

The content of any document created as a part of a staff member's school role remains the professional responsibility of the person who produced it.

- Any plans, policies or documents created using AI will be clearly attributed.
- Staff will only use approved AI tools for their professional work
- Staff will thoroughly check AI generated material for accuracy and bias before submitting it as a finished document.

Bias and Error

We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought will be applied to all outputs of authorised AI applications. This means fact and sense-checking the output. We will ensure we can identify and rectify bias or error by training staff in this area.

Please see the *Artificial Intelligence Policy* for more information and details of AI tools the school has currently approved for use by staff in their professional capacity.

Personal use of school ICT and Internet 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 be 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.

Social Networking

- 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

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

- The personal use of these services is strictly forbidden on school premises or on school equipment

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.

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.**

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

The school Remote Learning Policy gives detailed guidance on this aspect of ICT Security.

Key points for staff to remember include:

- Remembering to be particularly careful about posting images of children with identifying information
- 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

Staff Communication with Children

School staff should:

- not communicate/make contact or respond to contact with pupils outside of the purposes of their work.
- not give out their personal details.
- use only the equipment and internet services/platforms provided by the school or setting
- only use internet-enabled personal devices in line with school acceptable use policies.
- follow their school / setting's acceptable use policy and online safety guidance.
- ensure that their use of technologies could not bring their employer into disrepute.
- not discuss or share data relating to children/ parents / carers in staff social media groups..

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

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.

Use of Artificial Intelligence Tools

- I will only use agreed and approved AI tools to produce lesson plans, resources and materials for use with children.
- I will always attribute the use of AI when I use it in my professional work
- I will not use Generative AI with children in the classroom without getting permission from a member of the SLT.
- I will never input personal information that could identify a pupil or colleague into any AI tool or software.

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 or 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

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.

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

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 for home or remote learning 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 publishing content created by pupils and families on the website or social media 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

Full Name

Date

(printed)