



Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

What is an AUP?

We ask all children, young people and adults involved in the life of Roman Road Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school, Every time changes are made to the form.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Roman Road Primary School's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Samuel Stone, DSL, Samuel.stone@romanroad.newham.sch.uk

What am I agreeing to?

1. I have read and understood Roman Road Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).
3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
 - not sharing other's images or details without permission
 - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this [Online Reputation](#) guidance for schools and in Roman Road Primary School's Online Safety Policy.
9. I agree to adhere to all provisions of the school GDPR Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify DSI, Head Teacher if I suspect a breach. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
10. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an

education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

11. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
12. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
13. I will follow the guidance in the Online Safety Policy for reporting incidents – I understand the principle of ‘safeguarding as a jigsaw’ where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
14. I will not use my personal Mobile Phone during the school day (8:30-3:30) in any place but the staffroom, meeting room or PPA room. This includes within offices as well as Classrooms.
15. If I need to be contacted in an emergency I will direct people to call the school office to pass on a message. In some circumstances the Head Teacher or Deputy Head Teachers will permit the use of a personal phone but permission must be sought.
16. Whilst on school trips I will only capture images or videos of children using school IPADS and never my personal device. I understand that I can either use my own phone to contact school on trips or use a school phone. My use of the device is limited to contacting school and not for personal reasons.
17. I understand that breach of this AUP and/or of the school’s full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.



Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by DSL/ Deputy Head Teacher/ Head Teacher

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____

Name: _____

Role: _____

Date: _____

Admission granted for:

U Drive	
Google Drive- Shared	
USO	
SIMS- Register Takers	
SIMS- Full Access	
SIMS- Limited Access	
Printer Login	
WIFI	
Sign In System	
FMS	
WP- All	
WP- Folder Specific(Access granted to named folders)	
Other:	