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

Background

We ask everyone involved in the life of Nexus Education Schools Trust (NEST) 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 staff, local committee members (LCM) and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), LCM 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.

If you have any questions about this AUP or our approach to online safety, please speak to your Headteacher, Line Manager or the CEO.

What am I agreeing to?

1. I have read and understood NEST's full Online Safety policy www.nestschools.org 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 as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
3. I 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/Line Manager/CEO (if by an adult) and make them aware of new trends and patterns that I identify.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)
5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.
6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'! If I am unsure how to address any issues, I will seek support from the DSL.
7. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (eg. to take photographs of equipment or buildings), I will have the prior permission of the Headteacher (this may be delegated to other staff), and it will be done in the presence of a member of staff. The same principles apply for wearable technology. Smart glasses must not be worn in school. Please speak to your Headteacher if this presents any issue.

8. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
9. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
10. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
11. I will check with the Headteacher/Line Manager/CEO if I want to use any new platform of app that has not already been approved by the school, to ensure this is quality assured.
12. I will liaise with the Trust/DPO if I wish to use any AI technology and take into consideration the NEST AI Policy which lists approved platforms. I understand that a Data Protection Impact Assessment (DPIA) needs to be completed for the use of any new technology.
13. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.
14. I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness. I will flag any concerns about "overblocking" to the DSL (such as if I cannot access teaching materials).
15. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
16. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
17. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
18. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
19. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
20. 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 both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
21. 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/Line Manager/CEO

22. If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher/Line Manager/CEO of this as soon as possible.
23. 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 ever not sure, I will ask first.
24. I will not use any new technology or download any apps without agreement from the Headteacher/Line Manager/CEO.
25. I will not use a mobile hotspot to provide internet to any device I use in school.
26. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies www.nestschools.org at all times, whether or not I am on site or using a school device, platform or network.
27. I will never use school devices and networks/internet/platforms/other technologies 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.
28. 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. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here www.nestschools.org may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
29. I will only use AI platforms that have been authorised for use (including those used with pupils and to support administrative tasks), and I will ensure that any use of these platforms is transparent, responsible, appropriate, legal and ethical. I will ensure that I abide by all data protection legislation in relation to using these platforms.

Acceptable Use Policy (AUP) for
STAFF, LCM, 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		**Date**	
Name		**Role**	

To be completed by [insert here the name/s and role/s of the member of staff with delegated authority from the Headteacher/Principal to issue access/usage permissions]

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

Systems: [ie MIS, emails, Safeguard, CPOMS, PSF, network drives, etc]			
Additional permissions (e.g. admin)			
Signature		**Date**	
Name		**Role**	