



Acceptable Use Policy

Staff, Governors, Visiting Professionals, Volunteers



The Stour Federation

1. BACKGROUND

We ask everyone involved in the life of The Stour Federation Multi Academy Trust to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using Trust 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, governors and volunteers are asked to read, understand, follow and sign it when starting at the Trust and whenever changes are made. All staff (including support 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 Trust'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, it is your responsibility to please speak to the Designated Safeguarding Lead (DSL) in your school.

2. WHAT AM I AGREEING TO?

1. (This point is for staff and governors): I have read and understood The Stour Federation Multi Academy Trust'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. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
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.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way (by adults or pupils) to the Designated Safeguarding Lead (if by a child) or Headteacher (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 Child Protection Policy and Online Safety Policy 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. I understand that 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.
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. 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/in a locker/drawer and turn it 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. If required (e.g. to take photos of

equipment or buildings), I will have the prior permission of the Headteacher and it will be done in the presence of a member of staff. The same principles apply for wearable technology. Smart glasses should not be worn in school. I will refer to the Mobile Phone Policy and Smartwatch and Wearables Policy for detailed expectations regarding device use during contact time.

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.
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.
11. I will check with Christian Hilton, CEO (Trust Data Protection Lead) if I want to use any new platform or app that has not already been approved by the Trust, to ensure this is quality assured and a data protection impact assessment is undertaken. This includes any generative AI apps.
12. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.
13. I will prepare and check all online sources and classroom resources before using them, for accuracy and appropriateness (including ensuring adverts do not play at the beginning of videos).
14. 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.
15. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
16. During any periods of remote learning, I will not behave any differently towards pupils compared to when I am in school and will follow the same safeguarding principles as outlined in the main Safeguarding and Child Protection Policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
17. 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.
18. 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.
19. 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. I will not share others' images or details without permission and will refrain from posting negative, threatening or violent comments about others.
20. I will not contact or attempt to contact any pupil or to access their contact details in any way

other than school-approved and school-monitored ways, which are detailed in the Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.

21. If I already have a personal relationship with a pupil or their family, I will inform the DSL of this as soon as possible and update my social contact declaration.
22. 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, Staff Behaviour Policy (Code of Conduct), Smartwatch and Wearables Policy and Mobile Phone Policy. If I am ever not sure, I will ask first.
23. I will not use any new technology or download any apps without agreement from the Senior Leadership Team or the IT service provider, as outlined in the Online Safety Policy.
24. I will not use a mobile hotspot to provide internet to any device I use in school.
25. I agree to adhere to all provisions of the Trust's Cybersecurity and Data Protection guidance at all times, whether or not I am on site or using a school device, platform or network.
26. 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.
27. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I understand that any breach of this AUP and/or of the Trust's full Online Safety Policy or Staff Behaviour Policy (Code of Conduct) may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
28. I will only use AI platforms that have been authorised for use, which currently are Google Gemini, Microsoft Copilot and Oak National Academy Aila as approved by Warwickshire ICT Development Service. 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, specifically avoiding entering child data or sensitive information into generative AI systems.

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: _____

School and Role: _____

Date: _____

To be completed by the Headteacher / CEO

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

Systems: _____

Additional permissions (e.g. admin) _____

Signature: _____

Name: _____

Role: _____

Date: _____