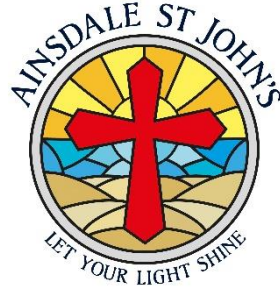# Acceptable Use Policy (AUP)
Staff, Governors and Volunteers

2024-2025

OUR TRUST PRAYER

Heavenly Father,

Let peace, friendship and love grow in our schools.

Send the Holy Spirit to give

excellence to our learning,

love to our actions and

joy to our worship.

Guide us to help others,

so that we may all

Learn, Love and Achieve, Together with Jesus

Amen

Background

We ask everyone involved in the life of our 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 staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. 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.

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

What am I agreeing to?

1. **(This point is for staff and governors):**
   I have read and understood school's full Online Safety policy (the policy can be viewed on our website) 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 (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'!
7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

8. 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/students).

9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils/students 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).

10. I will check with the curriculum lead if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured.

11. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.

12. 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.

13. I will carefully supervise and guide pupils/students 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.

14. I will physically monitor pupils/students using online devices in the classroom to ensure appropriate and safe use.

15. During any periods of remote learning, I will not behave any differently towards pupils/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.

16. 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.

17. If I am printing documents at home, I understand that for security reasons I must not use network printing and must plug in a USB cable.

18. I understand that I should not print anything of a sensitive or confidential nature at home.

19. I understand that Bitlocker encryption has been mandated for all devices including removable media. If I am concerned that my device/removable media is not Bitlocker encrypted, I will immediately report this to the Headteacher.

20. I will not store school-related data on personal devices, storage or cloud platforms. If necessary, I will only use the web browser to create and edit files and will not download a file to edit it (*the file could remain on an unencrypted drive*).

21. USB keys, if allowed, will be Bitlocker encrypted. I understand that only in exceptional circumstances will I be granted permission by the Headteacher to use encrypted USB keys and I must be able to fully outline and justify the reason for use.

22. I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times. I will not install software without seeking permission of the Headteacher (depending on my role, I understand that I may not have access rights and/or authority to install any software).

23. 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 that pupils/students 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.

24. 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.

25. I will not contact or attempt to contact any pupil/student 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/students to do the same to the headteacher.

26. If I already have a personal relationship to a pupil/student or their family, I will inform the DSL/Headteacher of this as soon as possible.

27. 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 and Data Protection Policy. If I am ever not sure, I will ask first.

28. I will not use any new technology or download any apps without agreement from the curriculum lead.

29. I will not use a mobile hotspot to provide internet to any device I use in school.

30. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.

31. 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.

32. 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.

33. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

34. I will only use gen AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

To be completed by the user

I have read, understood and agree 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 the Headteacher

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

Systems:

LDST systems e.g. Outlook for email, calendar, Sharepoint, OneDrive

Where applicable for teaching staff: SIMS for register and contact information, CPOMS for safeguarding concerns, Class Dojo for communication with parents, BSquared for measuring progress of children with SEND, Insight/AskEddi data system, curriculum websites as set out in curriculum document (SLT are admin and will add those this is relevant to)

Signature:

Name:

Role:

Date:

Review Schedule

Policy Author	Data Protection Officer (DPO)
Policy Approver	Trust Corporate Services Director
Current Policy Version	1.5
Policy Effective From	1st September 2024
Policy Review Date	By 31st August 2025

Revision Schedule

Version	Revisions	By whom
1.0	Original document produced	DPO
1.1	Updated in line with KCSIE 2020 and COVID-19 (insertion of new points 3, 4 and 6; deletion of previous point 4 and 8; point 5 significantly updated with reference to RSHE curriculum; point 11 password requirements added; all other points reviewed, some with minor amendments made).	DPO
1.2	Reviewed in line with KCSIE 2021. Bullet points 9, 17 and 19 have been amended. New Bullet Points 13-18. Bullet 11 now separated to create Bullet 11 and 12.	DPO
1.3	Reviewed in line with KCSIE 2022. New bullets 3 and 4. Bullet 5 and 6 amended. New Trust Prayer.	DPO
1.4	Reviewed in line with KCSIE 2023. New bullets 4, 5, 8, 9, 10, 11, 12 and 21 (filtering and monitoring responsibilities, professional curiosity, supporting pupils with their online knowledge and behaviour)	DPO
1.5	Reviewed in line with KCSIE 2024. New bullets 10, 14, 26, 28, 29 and 34.	DPO