AUP (STAFF): ACCEPTABLE USE POLICY FOR ICT

Date	Changes
Sept 2025	Reviewed by Anton Steinhardt

Review date: 1st May 2026

All staff are required to read the following document and sign by way of agreement. This is effectively an aide memoire. For further guidance on your legal obligations and for advice in dealing with any ICT related issue please contact IT Support. For each of these rules, the Headteacher reserves the right to grant permission in individual cases and to investigate any potential breach of these rules under the appropriate policy.

1. **I will ensure that I comply with the requirements of GDPR** *based on the guidance that has been provided and is accessible on the website (Data Protection Policy) and if in doubt will speak with the school's Data Protection Officer for guidance.*

2. **I will keep all passwords secure and request that students do the same.** *Never share passwords. If you suspect someone knows one of your passwords, change it immediately. Other than in cases of hacking, you remain responsible if others log in to any site using your username and password. Nobody must use your device if it is logged into your account*

3. **I am aware that if I choose to use any personal device, memory stick or storage device then this must be protected by either a password known only to me or biometric.** *I accept that using an email app, ICT staff could be given written authorisation by the Headteacher to reset my phone to factory settings deleting all personal data on it. ICT staff do not have any access to phone data and can at no time see what the phone is being used for. I will ensure any device used is up to date with anti-virus protection. We reserve the right to refuse connectivity of personal devices to our network or connected services.*

4. **I will lock or log out of any device if left unattended and request students do the same.** *Press CTRL + ALT + DELETE and choose to 'Lock my computer' / ⊞ L/or close the lid of a laptop if you leave a device unattended. Confidential information such as SIMS and emails must not under any circumstances be accessible by students. Any confidential information printed out must be protected and finally shredded.*

5. **I will return all IT equipment to a locked cupboard or to IT support when not in use.** *We cannot claim insurance for IT equipment which is taken WITHOUT forced entry. If you see any IT equipment that could be taken without forced entry you should secure it. You may be expected to pay towards repairs or replacement if damage is caused by lack of reasonable care.*

6. **I will not contact a student using my personal phone or give a student my number.** *A 'School' phone is a mobile or line owned and monitored by the school and should be used. Personal mobile or phone numbers MUST NEVER be given out or used unless the safety of the student is directly at risk (in such cases, senior staff should be informed at the earliest opportunity and any record of the number removed from the device).*

7. **I won't endorse students, staff, Trustees, Members or Governors use of personal email accounts.** *Governors, staff and students are issued with a school owned email account and this is the one that should be used without exception.*

8. **I understand that email is a written record and copies can be requested.** *I will always be polite and not include inappropriate or derogatory content. I will take time to check who I am sending to and will not add in new recipients before considering the whole past trail.*

9. **I won't cause a data breach or potential data breach by accessing, attempting to access, or sharing data (including personal data)** *to which I am not permitted to have access, or without authorisation.*

10. **I must take extra care when sending sensitive or confidential information by email**. *Any attachment containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.*

11. **If I receive an email from an individual or company that I do not recognise or expect to receive the communication from, I should refer this to the Data Protection Officer/ IT Services Manager for review.** *I will not open any documents/links attached or embedded within such an email without verifying the content accordingly.*

12. ***I will report any suspected cyber security incidents to the IT Services Manager*** *as a matter of urgency. These could take the form of phishing or suspicious emails, unsolicited phone calls where personal information is requested or suspicious looking websites.*

13. **I won't remove, delete, transfer, share or dispose of the School's ICT equipment, systems, programmes or information** *without permission of authorised personnel.*

14. **I will only ever use 'school' online accounts to contact any student directly or post ANY information relating to my role in school.** *A 'school' online account is any social media or other account owned by the school such as our email and O365 or any site which has been set up with at least two staff as administrators with full access, one a post holding teacher. You must lock down your personal account so that only minimal information can be accessed by students. Posting of any student work or images must only ever be on a school owned site and even then, only with signed consent. Ask for specific advice about any site.*

15. **I will enforce the student AUP correctly to help keep children safe.** *We want to encourage students to use ICT in responsible and safe ways, this is everyone's responsibility.*

16. **I will never use working hours for any personal IT use.** *All staff can use school IT equipment on site and off site including at home. During school hours, IT cannot be used for personal browsing, personal shopping, personal gaming, personal advertising through SMART email systems or personal social media. Accessing material unsuitable for use in schools due to offensive or adult rated content on a school device at any time may lead to disciplinary measures.*

17. **I will never knowingly infringe copyright or endorse or encourage others to do so.** *It is your responsibility to make sure that any audio, video, images, text or software you use is not in breach of copyright.*

18. **I understand that any files or media created, uploaded or downloaded using school software, network or equipment remains the property of the school and may be monitored or withdrawn at any time without notice.** *For additional security, if it is felt necessary to view your history or files without your permission then this will only be done by the IT Services Manager under direct request from the Headteacher or Leadership Team member in charge of E-Safety.*

19. **If I become aware of any member of staff accidently breaking the conditions of the AUP I will immediately bring it to their attention. If the situation is not remedied, I will inform a senior leader.** *Our normal procedure would be to discuss the issue at the first opportunity and to assume a genuine error had occurred.*

20. **If I become aware of any member of staff knowingly breaking the conditions of the AUP I will immediately bring it to the attention of the Headteacher/Data Protection Officer.** *This would be investigated under the appropriate policy.*

21. **I understand E-Safety is everyone's responsibility and I will regularly role model safe use and enforce the use of the student AUP.** *Encourage students to use ICT wherever it helps learning and keep trying new approaches so they can benefit fully, but at the same time ensure they follow rules to keep them safe.*

22. **I understand images or videos of staff or students can only be shared if the subjects have authorised it.** *Parents are asked each year for their authorisation. Any copies not shared (e.g. in a shared drive) must be deleted at the earliest opportunity.*

23. **I understand that I must not record images or video recordings of staff or students on a personal device**. *I will use a school device (camera/ ipad/ phone) that is allocated for that use and follow the procedures accordingly.*

24. **Where the school uses social media accounts, staff members who have not been authorised to manage, or post to, those accounts, must not access or attempt to access these accounts.**

25. **I will discuss with, and seek approval from, relevant staff on the potential use of AI in the creation of any resources or materials for use in school.** ***Including approval for the use of specific AI tools and applications.***

26. **I will not enter personal, sensitive or identifiable data into any AI tool or application as it may represent a breach of our Data Protection policy.**

Name _____

I confirm I have read this AUP _____

Date _____