Name of School	**Spa School Camberwell**
AUP review Date	**September 2021**
Date of next Review	**September 2022**
Who reviewed this AUP?	**Georgina Quigley/ Steph Lea**

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by Spa Education Trust.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow students to access systems using my login.
- I will not allow students to access the internet without adult supervision and will restrict access to the internet for approved use only
- I will not allow unauthorised individuals to any school system.

- I will ensure all documents and data are managed in accordance with the whole school policy and in accordance with GDPR regulations.
- I will report any data breach to Simon, Georgina, Nusrat or Steph immediately

- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will record all e mail communication with parents/carers on CPOMS
- I will not share my personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business
- I will follow school guidelines on confidentiality of any information about pupils.

- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the SMT.
- I will not download any software or resources that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright or breach intellectual property rights.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network that does not have up to date anti-virus software, and I will keep any 'loaned' equipment up to date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.

- I will ensure any private online communication I create or contribute to, is not confused with my professional role.
- I will ensure that my social media presence is not linked to the school, that my work e mail is not linked to my accounts and that my privacy settings are checked regularly.
- I will not engage in any online activity that may compromise my professional responsibilities.

- I agree and accept that any computer, laptop or iPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely only through school approved methods and follow security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, such as Egress Switch, and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's online safety curriculum into my teaching.
- I will alert the SMT and/or safeguarding lead if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the designated safeguarding lead.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up to date and read and understand the school's most recent Privacy Notices, Online Safety and Data Breach policies.

Signature ....Date ....

Full Name .... (printed)

Job title ....

Social Media Safety Top Tips

10 rules for school staff on Facebook and other Social Media platforms

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- On Facebook, change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- Consider changing your Instagram account to Private
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that you have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening straight away

You’re being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- Notify the senior leadership team or the headteacher about what’s happening straight away
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Taken from Cheat Sheet for Staff: The Key Support Services