Acceptable Use of IT Policy – Staff and Governors

Radnor House asks all children, young people and adults involved in the life of the 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).

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, Remote Learning Policy, and the other relevant school policies (e.g. Safeguarding Policy, Staff Code of Conduct, Behaviour Policy, etc.).

This AUP is reviewed annually, and staff, directors and volunteers are asked to sign it through the school's HRIS upon entry to the school, at the beginning of each academic year and any time changes are made.

If you have any questions about this AUP or our approach to online safety, please speak to Dan Cater, IT Manager, or Simon Jay, DSL and Head of Online Safety.

AUP:

I have read and understood Radnor House's full Online Safety (and, for teaching staff, Remote Learning) policies 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.

I understand it is my duty to support a whole-school safeguarding approach and 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 Principal (if by an adult).

I understand the responsibilities listed for my role in the school's Online Safety Policy (staff, please note that the 'All Staff' section applies as well as any other category) and agree to abide by these.

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, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

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.

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 not sure if I am allowed to do something in, or related to, school, I will not do it and will check with the Head of Online Safety, who is also the Designated Safeguarding Lead.

I understand the importance of upholding my online reputation, that of the school and of the teaching profession, and I will do nothing to impair either. More guidance on this point can be found in the school's Staff Code of Conduct.

I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/ other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/ or relevant/authorised staff members.

I understand that the filtering/monitoring software solutions used by the school are not used as a means to spy routinely on users. They may though be used for investigative purposes, should the need arise. Although the ability exists for any IT support personnel to be able to view another user's screen and potentially read confidential emails/documents, the school has put safeguards in place to protect users as well as the IT support team.

I agree to adhere to all provisions of the school's Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the IT Manager if I suspect a breach. I will ensure my desktop screen is locked while away from the monitor for any period of time. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

I will use school devices and networks/internet/platforms/other technologies for school business only, and I will never use these 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 I will look after school devices loaned to me.

I will only use those systems, apps, IM communication tools (i.e. MS Teams), etc. adopted for use by the school, for school/work-related matters.

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 by the school. For further information, please see the school's Safeguarding and Preventing Extremism and Radicalisation Policies.

I understand and support the commitments made by pupils, parents and fellow staff, directors and volunteers in their Acceptable Use Policies, and I will report any infringements in line with school procedures.

I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might consider to be unimportant. I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handing incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.

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

I understand that my current and historic email communication to/from my school email address belongs to the school, and I understand that, when I leave my position at the school, the school may need continued access to my school emails and system to ensure the continued smooth-running of the organisation.

As per the point above, I understand that any written communication on other school systems belongs to the school, and the school will have continued access to these when I leave my position at the school. I understand that personal documents should not be stored on MS Teams.

I understand that, under data protection legislation, staff must not remove any personal information from previous schools/employment and store it on the school system at Radnor House. To remove such information on leaving a place of employment is illegal and can result in prosecution.

By confirming that I have read, understood and agreed to this policy on the school's HRIS, I understand that it is also my responsibility to ensure I remain up to date and read and understand the school's most recent Online Safety and Safeguarding Policies. I understand that failure to comply with this agreement could lead to disciplinary action.

September 2023

Appendix – School Computer Log-In Agreement

Whenever anyone logs in to a school computer or device, these bullet points appear on the screen, which all users must accept before continuing.

By using the school network, I agree to the following:

- I will only use electronic devices in school for school purposes and will not use them for personal or recreational use unless I have permission to do so.
- I will handle all computer equipment carefully and will not touch power/network cables or eat and drink in the IT suites.
- I will not use disks, memory sticks or any other hardware with school equipment without the permission of my teacher.
- I will not download or install software on school technologies.
- I will only log on to the school network and other systems with my own username and password.
- I will not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all electronic communications with pupils, teachers or others is responsible, polite and sensible.
- I will not deliberately browse, save or send material that could be considered offensive or illegal, if I accidentally find anything like this I will tell my teacher immediately.
- I will not give out any personal information such as my name, phone number or address.
- I will ensure that my online activity, both in school and outside school, will not cause distress to my school, the staff, pupils or others.
- I will not attempt to bypass the Internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers If I see any misuse of computers I will report it to a teacher.
- Personal computer equipment can only be used on school premises with the permission of the school and on signature of the Radnor House Bring Your Own Device (BYOD) Policy.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my, parent/carer may be contacted.