TECHNOLOGY ACCEPTABLE USE POLICY FOR STAFF

The purpose of the policy is:
- To outline the acceptable use of computer equipment at Farnborough Hill.
- To put in place rules to protect both the user and Farnborough Hill.
- To safeguard the system from potential threats such as virus attacks, hacking, system failure and breach of legal requirements.
- To raise staff awareness of their duty to use Farnborough Hill's digital resources for professional purposes responsibly, ethically and lawfully, and to ensure their pupils do the same.

All staff need to be aware that:
- The Director of Digital Infrastructure and Senior Leadership Team reserve the right to access files, folders, network data and workstations at any time, with reasonable cause.
- Farnborough Hill filters, monitors and records all device usage and activity both in school and on school cloud based software. This includes the use of the internet as well as general network usage. Staff may request that certain sites be temporarily 'unblocked' if this will assist their teaching.
- Staff will have access to Farnborough Hill digital resources (including their email account) until the final day of their employment by the School.
- External storage devices such as USB sticks are not permitted in school for network security reasons. If you have any concerns about the provenance of an email, do not open it, rather delete it and report it to IT Support.
- This policy should be read in conjunction with the School's Safeguarding Policy.

Staff need to:
- Be fully aware of the contents of the Technology Acceptable Use Policy for Pupils and do everything they can to ensure it is upheld.
- Use the network and all computer equipment appropriately and responsibly.
- Report any loss or damage to computer equipment to the Director of Digital Infrastructure or a member of the IT Support Team.
- Contact a member of the IT Support Team if any resource behaves unexpectedly.
- Be aware that if they install software on a home computer which is licensed through the School, it is their responsibility to uninstall it when they leave the School's employment.
- Be responsible with the amount of storage space used, and to undertake regular 'housekeeping' to delete unwanted files.
- Take care when choosing passwords in order to keep the School's systems secure. Carelessness when choosing passwords leaves confidential pupil data vulnerable to theft. Passwords should be updated at the beginning of every term and should contain a mixture of alphabetical, numeric and special characters. We recommend that you change your password at the beginning and end of each holiday to avoid being locked out of school systems.
- Ensure that printing is carried out in a responsible and economical fashion. Where possible use iPads or other electronic means to view documents rather than printing hard copies. When printing is required, duplex monochrome copies should be used. Colour printing should only be used in exceptional circumstances. All printing for classroom use should be sent to reprographics in good time. Personal printing is not permitted.
- Ensure that if they use generative Artificial Intelligence (AI) to assist with their work they most follow all guidance in the School's Generative AI Policy.

Staff must take care not to:
- Harm, offend or bully anyone using technology.
- Procure, display or distribute any material that may be illegal, harmful, offensive or detrimental to anyone. This includes, for example: racist or extremist material, material of a sexual nature and viruses.
- Engage in any illegal activities.
- Make any sort of recording, whether audio or visual, of any conversation or meeting with anyone in the School community without their express permission, as so doing would constitute a breach of trust.
- Log on using another person's username and password, attempt to access another person's files or data or give out any usernames or passwords.
- Give out, or publish, personal details relating to any member of the School community without permission.
- Take part in any activity that may be detrimental to the School's name, at home or in school.
- Install or run any unapproved or unlicensed software/programs on any school computers, laptops or iPads.
- Change any of the configuration settings of any school computer, laptop or iPad.
- Provide access to copyright works beyond that which is allowed under current copyright legislation.
- Whilst in school, use personal devices – whether using the School Wi-Fi network or their own provider's 4G or 5G network, including mobile, hand-held and tablet devices, in a way which contravenes this policy.

Electronic communications:
- Staff must not contact or communicate with any pupils or parents or carry out any school business using personal social media accounts such as Facebook.
- Professional messaging groups, such as Microsoft Teams should only be set up and managed by a member of staff for school business such as extra-curricular activities and clubs. These groups should remain unlocked and should be actively monitored and managed by the member of staff responsible. Personal messaging groups such as what's app should not be used for school activities.
- Communication via email with pupils in years 7-9 is discouraged except in exceptional circumstances. If staff members are contacted by a pupil for support they should arrange to see them in person in the first instance. Firefly, OneNote and Teams are the only platforms that should be used to set work for or communicate with pupils in Years 7 - 10 either individually or in groups.
- We recognise that staff may at times work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks, iPads or personal devices. We authorise such occasional use [provided use is minimal and takes place substantially out of normal working hours (ie during lunch break or before or after work) and] so long as it does not involve unprofessional or inappropriate content, does not interfere with employment responsibilities or productivity.
- Staff must maintain the securest settings on any personal social media sites, so that pupils, parents, former pupils and others cannot see any personal information. Staff should not become 'Friends', 'Follow' or make direct connections on any social media sites with present pupils. This also applies to ex-pupils until they are 18 and have finished secondary education. In addition, they should not seek to view any pupil's social media. The only exception to this rule would be if specifically requested to do so by the DSL or Head, and only then in the course of investigating a discipline or safeguarding matter. Staff are strongly advised to use these sites in a professional manner and, should any concerns arise, they should seek the advice of the Head as soon as possible. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the School's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.
- Permission to use the School's systems to access social media platforms for personal use may be withdrawn at any time at the School's discretion.
- Staff must not engage in personal on-line conversations using the School network, or access Instant Messaging sites or chat sites for personal use whilst in school.

- Staff should not respond to parent enquiries that are received via email other than to acknowledge their receipt via the School office. Communication with parents is better taking place via telephone where misunderstandings are less likely. Only Heads of Year, Heads of Department and Senior staff will communicate with parents by email.

When using email:
- A 'Farnborough Hill' email address will be provided to all staff and is part of the School's digital infrastructure. It is therefore subject to the same conditions as those laid out in this Technology Acceptable Use Policy. This email address should be used for all work-related email.
- The use of all other personal email accounts, such as Hotmail and Gmail should not be used for school business.
- Do not open unknown email attachments.
- Best practice for email usage is during school opening hours (7.30 am – 6.00 pm) for both internal and external communication. If composed outside of these hours please automatically schedule them to be sent during these hours or save to drafts and send the following day.
- Staff should not set up any kind of service to forward school emails to a personal email account, to do so would be in breach of the General Data Protection Regulations (GDPR).
- Staff members wishing to set up a personal device to receive school emails should ensure that the device is not accessible to anyone else (eg family members). It is strongly recommended that a separate application is used for school emails (eg Microsoft Outlook) to ensure that they are kept separate form personal mail. Appropriate security (strong passwords or biometric protection) should be used to ensure the account remains secure. Any loss or theft of a personal device that grants access to a school email account should be reported immediately to IT Support Team and the Bursar.

When accessing the network from outside the School staff must not:
- Transfer any material that could be deemed offensive, harmful or illegal from outside the School to the School network. This includes transfer by Internet or by any form of removable media.
- Share any confidential or whole school documentation, such as that on the Staff Shared drive, with anyone from outside the School.
- Transfer or store any confidential information on cloud services such as Dropbox or GoogleDrive. The only cloud storage that may be used is the School provided OneDrive account.

When using a laptop provided by the School staff must:
- Adhere to this policy, as above.
- Store the School laptop in an appropriate manner minimising the risk of theft or damage. If left in an unattended motor vehicle it must be concealed in a locked boot.
- Not install programs for which the School does not have a valid licence.
- Return any borrowed laptop to school promptly.

When using an iPad provided by the School staff must comply with the following:
- Adhere to this policy, as above.
- The iPad must must remain in the possession of staff, should only be used by them and should be securely stored when not in use. All associated items, including the charging cable and Apple Pencil (if issued), should be kept in good order. Staff must be mindful of the agreement they signed when their iPad was issued and ensure that any loss or damage should be reported to the Director of Digital Infrastructure.
- If staff leave the employment of the School, or have an extended leave of absence eg for maternity/paternity leave, then the iPad must be returned to IT Support prior to their official leaving/period of absence date.
- Personal photographs or video should not be stored on the iPad.
- Where photos or videos have been taken of pupils using a school iPad for the purpose of teaching and learning these should not be retained for any longer than absolutely necessary.
- Any confidential pupil data stored on staff's iPads must be deleted once it is no longer needed.
- Staff iPads are configured by the School Mobile Device Management System. Staff must not attempt to change these settings or remove it from the Management System. VPN (Virtual Private Network) apps must not be used.

- Staff iPads are set up to require a complex passcode and to lock automatically after two minutes of inactivity. This setting must not be changed.
- Staff must purchase and use an appropriate cover to protect their iPad while it is in their possession or use the one provided by the School. (If a specific case has been provided this must be used)
- Activate iCloud to ensure that data remains safe in the event of loss or damage to an iPad.
- Insurance cover provides protection from the standard risks whilst the iPad is on the School site **but excludes** theft from a staff member's home, car or other establishments. Should the iPad be left unattended and it is stolen, staff will be responsible for its replacement.
- Remember that any connection cost incurred by accessing the internet from outside school is not chargeable to the School.
- iPads may be checked periodically for safety and compliance with school policies. Outcomes will be reported to the Head.
- Free Apps may be downloaded to staff iPads for educational purposes at any time. However, staff may have to provide their own credit card details in order to do so. If staff do not wish to do so, then free Apps can be sent to staff iPads via the Mobile Device Management System. Staff should contact IT Support to facilitate this.
- Paid Apps should be purchased through the School by completing the relevant form on Firefliy. Any Apps purchased by staff independently of this will not be reimbursed. When requesting that an App be purchased, authorisation should be sought from the relevant Head of Department. The cost of purchased Apps will be taken from departmental budgets.
- Social Networking Apps should not be downloaded or installed, unless for a specific and authorised purpose.

This policy is reviewed annually by the Director of Digital Infrastructure in conjunction with the Deputy Head – Operations.

The next review is due in October 2025.