FARNBOROUGH HILL
WHOLEHEARTEDLY

ICT 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 ICT resources for professional purposes responsibly, ethically and lawfully, and to ensure their pupils do the same.

All staff need to be aware that:

- The IT Manager 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 ICT 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 ICT 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 ICT Acceptable Use Policy for Pupils and do everything they can to ensure it is upheld.
- Use the network and all ICT equipment responsibly.
- Report any loss or damage to ICT equipment to the IT Manager immediately.
- Contact a member of the IT Support staff 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 ICT 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.

Staff must take care not to:

- Harm, offend or bully anyone using ICT.
- 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.
- 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 ICT equipment – whether using the School Wi-Fi network or their own provider's 3G or 4G 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. Firefly is the only platform that should be used to set work for or communicate with pupils in years 7-10 either individually or in groups.
- 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 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. 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.
- 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 ICT resources. It is therefore subject to the same conditions as those laid out in this ICT 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.

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 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, should be kept in good order. Loss or damage should be reported to the IT Manager immediately.
- If staff leave the employment of the School, or have an extended leave of absence eg for maternity/paternity leaver, 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.
- Staff iPads are set up to require a six-digit 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 an STM Dux 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 Assistant Head in conjunction with the Director of ICT.

The next review is due in October 2019.