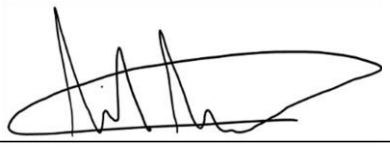
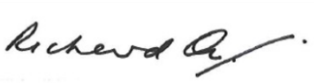
Name	IT Acceptable Use Policy
Version	V1.1
Author	Mikael Meoli (Head of IT Services)
Approver	Richard Quinn (Bursar)
Date	02/02/2018
Review Date	01/02/2019

Written By: 

(Signature)

Mikael Meoli, Head of IT Services

Approved By: 

(Signature)

Richard Quinn, Bursar

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that everyone working within the school is aware of their professional responsibilities when using any form of ICT.

The Acceptable Use Policy is also there to assist the staff in staying safe and to protect the security and integrity of the school's ICT systems.

All staff, governors and visitors using ICT within school are expected to sign this agreement and adhere to its contents at all times. Any concerns or clarification should be discussed with Danes Hill E-safety coordinator or Head of IT Services as appropriate.

The Agreement: -

- I appreciate that ICT includes a wide range of systems, including but not limited to mobile phones, digital cameras, tablet computers, eBook readers, email, social networking and that ICT use may include personal devices when used for school business. I understand that any personal equipment brought into school remains my sole responsibility and may only be connected to the school network with the explicit permission of the ICT department who may ask to check the device periodically for adequate Anti-Virus software. Permission will not be given if the device is not using a locking system requiring a suitable password or code to access it.

- I understand that the use of the school's systems outside of school is also covered by this agreement e.g. email, laptops, VLE etc.

- I will only use the school's ICT for professional purposes or for uses deemed appropriate by the Head or Governing Body.

- I will not use the school's internet connection for any purpose that will have an adverse impact on other members of the school community carrying out their work satisfactorily e.g. uploading, downloading large files or streaming content. Prior arrangement with the ICT department will usually mean that required content can be safely downloaded and stored for use when required.

- I will comply with the ICT system security and not disclose any passwords required by any of the programs or systems that I use. If I have any reason to believe that a password has been compromised I will immediately change it or if this is not possible, ask for a new one to be issued.

- I understand that I am responsible for all activity carried out under my username and that my usage will be monitored and logged. Such logs will be available on request to my line manager or Headmaster, or the governing body, and may be shared with the appropriate authorities if illegal activity is indicated or suspected. Logging on as another user is strictly prohibited.

- I will ensure that all computers and devices are logged off, shut down or locked at any time when I am not present.

- I will ensure that all electronic communications with students and staff are compatible with my professional role and such communications with students will only take place via a school email address or from within the Virtual Learning Environment and cannot be misunderstood or misinterpreted.

- I will only use the approved, secure email systems for any school business. School email addresses are for educational and professional use only.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headmaster or the Governing Body.

- I will not install any hardware or software without the permission of the Head of IT Services or Assistant Network Manager to ensure that the addition will not have an adverse effect on any existing programs or system performance.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, discriminatory, or contrary to the school's child safeguarding policy

- IT Resources purchased by Danes Hill School remain the property of the Vernon Educational Trust and can be taken down, removed or monitored and recorded at any time without warning by the Head of IT or Senior Management. The school uses monitoring software called lmpero to capture and monitor use of Danes Hill IT systems.

- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with the written consent of the parent, carer or staff member. Images will not be distributed outside the school network/ VLE without the permission of the parent/carer, member of staff or Headmaster.

- I will respect copyright and intellectual property rights.

- I understand that it is the school policy to have a password that conforms to the complexity requirements and that the password must be changed every three months. I understand there is also an auto lock policy in place that will lock admin machines after 5 minutes of inactivity and teaching machines after 40 minutes.

- It is the responsibility of the member of staff using information relating to the school to keep data used secure. This includes backups from iPads or other devices to data centers. It is forbidden to back up any data to locations outside of the UK.

- I understand that I must encrypt data that leaves the school premises. This includes memory sticks and data sent via email.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role, the School, or the Vernon Educational Trust into disrepute.

- I will report any incidents or concern regarding children's safety to the E- Safety Coordinator, the Designated Safeguarding Lead (DSL) or Head Master.

- I will report any damage to or malfunction of any ICT equipment that I attempt to use to the ICT department however it was caused and regardless of whether it had already occurred to ensure that all equipment is kept available for use.

- I am responsible for making sure that any device inclusive of personal computers, tablets, mobile phones and storage devices that have access at any time to the Danes Hill network have up to date virus protection at all times.

- I will support the school's E-safety policy and help students to be safe and responsible in their use of ICT and related technologies. I will promote E- safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will not uninstall any program or piece of software that is already installed or to be installed in the future on any Danes Hill owned device.

- I will not try to bypass any security or monitoring system installed by the organization. Doing so will be seen as a direct breach of this policy and will lead to disciplinary action.

- I understand that although filtering and monitoring of the school's network is in place I am responsible for any student use of the system whilst in a lesson or whilst I am the responsible adult.

- I will not leave any student unattended in any of the designated computer suites or in areas where student have access to Danes Hill computing equipment. This is inclusive of desktop computers, laptops, netbooks and tablets.

- I will conform to all IT security policies put in place by the Head of IT Services

The below applies to, but is not limited to loaned equipment (including smartphones):-

- Users must use protective covers/cases for the device where provided.

- The device screen is made of delicate material and therefore is subject to cracking and breaking if misused: Never drop or place heavy objects (books, laptops, etc.) on top of the device.

- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the device screen.

- Do not subject the device to extreme heat or cold.

- Do not store or leave the device unattended in vehicles.

- The device is subject to routine monitoring by Danes Hill School. Devices must be surrendered immediately upon request by a member of IT staff.

- Users in breach of the Acceptable ICT Use Policy or Loan Agreement may be subject to but not limited to: disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

- Danes Hill School is not responsible for the financial or other loss of any personal files that may be deleted from any device.

- If the device is lost, stolen, or damaged, the IT Staff must be notified immediately.

- Accessing Inappropriate Materials- All material (video, audio, images or text) on the device must adhere to the Acceptable ICT Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

- Illegal Activities- Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity is strictly prohibited.

- Violating Copyrights- Users are not allowed to have illegally sourced software or data on the device

- Cameras- Users must use good judgment when using any camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation and will lead to disciplinary action

- Misuse of Passwords, Codes or other Unauthorised Access: Users are encouraged to set a passcode on the device to prevent other users from misusing it. This passcode must be divulged to IT Support for regular maintenance and or updates.

- Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.

- Malicious Use/Vandalism- Any attempt to destroy hardware, software or data will be subject to disciplinary action.

- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary action.

- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.

- Users should be aware of and abide by the guidelines set out by the School eSafety policy.

IT Acceptable Use Agreement Form

Please complete and return this form to the Head of IT Services

Name:

As a school user of the Internet and SchooliCT equipment, I agree to comply with the school rules on its use and all terms highlighted in the IT Acceptable Use Policy. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

I understand that when using personal devices within school while connected using a Data Roaming Service or wireless connection not provided by the school, I must exercise particular care to ensure that I do not access unsuitable material. Should the school become aware, through monitoring or by any other means of such use, it will lead to disciplinary action.

Signature:

Date: