March 2017

Mobile Device Acceptable Use Policy 2017-18

Whole School

Contains relevant information on the practice and procedures of using I Pads or any other mobile handheld device used within school.

Table of Contents

Page …… 3

- Potential Benefits of Mobile Technologies.
- Responsibilities.
- Safeguarding and Maintaining as an Academic Tool.

Page…….. 4

- Lost, Damaged or stolen mobile devices.
- Prohibited Uses (not exclusive).

Page……..…… 5

- When personal devices are permitted.

Amendment's made on 23/3/2017

Page 3

- Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

- Responsibilities

Pro-active monitoring has been implemented to monitor activity, each class teacher has a mobile device folder to monitor and record the use of mobile devices within the school setting.

Page 4

- Lost, Damaged or Stolen mobile device.

If the mobile device is lost, stolen, or damaged, the computer co-ordinator or senior member of staff must be notified immediately, with a mobile device incident form obtainable from the school office.

- Prohibited Uses (not exclusive)

If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Head Teacher. The E Safety concerns form is located in the school office and must be filled in and returned to the computing coordinator or directly to the head teacher and recorded in the e-Safety log.

Page 5

- When personal devices are permitted (Whole section)

Mobile Device Acceptable Use Policy
January 2017

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

The policies, procedures and information within this document apply to all iPads, or any other IT handheld device used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

Responsibilities

- All mobile devices must use the protective covers/cases.
- The mobile device screen is made of glass and therefore is subject to cracking and breaking if misused: Never leave mobile devices on the floor or unattended, do not drop or place heavy objects (books, laptops, etc.) on top of the mobile device.
- Do not subject the mobile device to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that persons' consent.
- If a member of staff does not wish to have their photograph taken must inform Mike/designated photographer so they are aware of who does not wish to have their photograph taken.
- School cameras that are taken off site must have a clear sd card and one member of staff named on the risk assessment to be responsible for the safe keeping of the camera and all photograph's that have been taken.
- The mobile device is subject to routine monitoring by Stanley School. Devices must be surrendered immediately upon request by any member of staff.
- Users in breach of the Responsible Use Policy 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.
- Pupils must not use the mobile device outside of School buildings (without the Head Teachers' prior permission).
- Pro-active monitoring has been implemented to monitor activity, each class teacher has a mobile device folder to monitor and record the use of mobile devices within the school setting.

Safeguarding and Maintaining as an Academic Tool

- Syncing the iPad to iTunes or iCloud will be maintained by a School administrator.
- Changing the internet / proxy settings in school is NOT permitted as this will stop the profile management settings from working, this is maintained by the School administrator.
- The staff do not need to update apps as this is done from within profile manager.
- Installing or delete apps from the iPad will be maintained by a School administrator, school staff members are NOT permitted to do this.
- The staff can manually update the iOS if they need to.
- If they need to use the mobile device at home they can put in their own wireless details.
- All mobile device batteries are required to be charged above 40% and be ready to use in school.
- Items deleted from the mobile device cannot be recovered.
- All mobile devices MUST HAVE photographs and video's stored on the gallery cleared daily if the pupils have been left unsupervised with a mobile device.
- All mobile devices MUST HAVE photographs and videos cleared weekly if it has only been used by Stanley School Staff. EYFS will clear images being used for Evidence for Learning ever two weeks.
- Blue communication iPads must be available for pupils to use and communicate within the classroom.
- Blue communication iPads should NOT have the internet, camera or anything other than Proloquo2go accessible to pupils.
- Allowed content for websites should be set to specific Websites Only and if a member of staff enters the password to allow websites that are not on the restricted list it must be for educational purposes.

- If iPads are being used regularly to manage a pupils behaviour, this should be included in the pupils individual behaviour plan.
- Youtube kids app is available on the mobile device to promote safer internet use by our pupils. This is only to be used for a limited period as a reward with supervision.
- Pupils who can NOT report inappropriate material should not be on the internet unsupervised.
- Restrictions and appropriate setting should be checked regularly by the class teacher.
- It is the class teacher's responsibility to keep their mobile device safe and secure.
- Mobile devices belonging to other classes are not to be tampered within any manner.
- If an mobile is found unattended, it should be given to the nearest member of staff, and left with the computer co-ordinator with a mobile device incident form.
- The whereabouts of the mobile devices should be known at all times.
-

Lost, Damaged or Stolen mobile device

- If the mobile device is lost, stolen, or damaged, the computer co-ordinator or senior member of staff must be notified immediately, with a mobile device incident form obtainable from the school office.
- iPads that are believed to be stolen can be tracked through iCloud.

Prohibited Uses (not exclusive):

- Accessing Inappropriate Materials – All material on the mobile device must adhere to the ICT Responsible Use Policy. Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Head Teacher. The E Safety concerns form is located in the school office and must be filled in and returned to the computing coordinator or directly to the head teacher and recorded in the e-Safety log.
- Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Cameras – Users must use good judgment when using the 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.
- Images of other people may only be made with the permission of those in the photograph.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Leadership team.
- Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.
- Misuse of Passwords, Codes or other Unauthorised Access: Teachers are encouraged to set a passcode on the mobile device to prevent other users from misusing it.
- 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.
- Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
- 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 actions.
- 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.
- Stanley School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Policy.
- Digital Literacy and e-safety is a whole school responsibility.

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.

Adult Users must read and sign below:

I have read, understand and agree to abide by the terms of the mobile device Acceptable Use Policy.

Name:

Signature:

Date:

I have read, understand and agree to abide by the terms of the E-safety Policy & Practice 2016-17

Name:

Signature:

Date: