Lingham Primary School

Policy for the use of mobile devices for learning and teaching both in and outside of school.

Approved by Governors: 27th June, 2017
Updated: June 2017
Review date: June 2018

Mobile Learning Devices Policy

Mobile Devices Include;

- iPods
- iPads
- Android Tablets
- Smart Phones
- Other devices with the characteristics below

Characteristics of Mobile Computing Devices

- Access to the Internet with sharing capability
- Audio/Photo/Video Recording
- Device specific Software – "Apps"
- Compatability with more 'traditional' computing devices

Uses for Mobile devices in School Situations

- Accessing information and resources via the internet
- Capturing information via multimedia (camera/sound recording)
- Processing, editing and presenting information
- Sharing Information with peers and others within school via Cloud services and Web 2.0
- Publishing to the web for more widespread audience
- Administration – registration etc.

Potential Benefits of mobile devices:

- Camera and Audio Recording facility for quick and easy pictures and sound recording provides fast information acquisition
- Handheld and light to carry
- Easy to share information with others in a group activity
- Facilitates shared learning and collaboration
- Facilitates mixing, remixing and synthesis of ideas and information
- Intuitive Touch Screen Technology for immediate 'natural' access without need for peripheral devices supported by Intuitive software Easily create and arrange multi-media content

Potential Risks/Issues to be managed

- Damage or loss due to handling
- Management of User/Purchasing accounts including e-mail
- Wireless access
- Synchronisation
- Power Management and Charging
- Security and Access to devices including offsite use
- Permissions for Images etc. to be used
- Off site Storage of content

Device Management

- All devices will be set up to synchronise with one 'management' computer or "Mother Ship"
- Only apps approved by the school will be loaded onto the device. Staff must not load apps onto the device using their own user accounts, or access their personal mail accounts via these devices
- This will allow apps to be managed effectively as well as allowing regular updates to devices to be handled through one channel.
- Power Management and Synchronisation will be via the ParaSynch Tray/Box which connects to the Mother ship via USB.
- All devices should be signed out of storage and returned after use and staff must ensure that they are left in a charging state.
- Staff can take devices off site for school trips etc and the school will be then responsible for loss or damage.
- If staff wish to take home a device for familiarisation purposes they must seek permission from SMT. It then is their responsibility if lost, stolen or damaged, and it is their responsibility to replace the device. (check your Home Contents insurance)
- By synching with one machine, all content produced on the devices can be transferred to the Mother Ship and thence to the network
- In addition all devices should be connected to the school wireless network and from there via a filtered connection to the Internet thus providing access similar to that enjoyed via desktop/laptop devices
- Individual Staff using the devices are ultimately responsible for ensuring that any work created on the devices is downloaded/saved and the devices cleared ready for the next user

User Accounts

- Because of the nature of such devices, software is purchased via the Apple App Store or the Android Marketplace or similar.
- The school has a password protected user account and an associated e-mail account that receives invoices/receipts for purchases via the account. Payments are made via a pre-paid top up card as and when. There should be no more than £16 maximum in the account (£1 plus £15 top-up)
- Only the designated persons will access this account and make purchases. Admin staff are able to access the accounts and e-mail in order to provide fiscal accountability.
- Passwords should be changed regularly

Permissions

As part of the general Internet Policy of the school, all pupils/parents permission is requested for photographs and video to be taken. The reasons for this need to be clearly understood by staff and parents, as the devices will inadvertently capture pupils in a photograph and video, and parents need to feel confident that such content is safely held. Any video or stills posted to the Internet will not allow specific identification of children, unless there is a clear reason and in that case further permission will be sought

Third Party Apps Accounts and Information Storage
Some apps require access to accounts- for example storage or hosting of created content. The details of these accounts should be kept confidential and passwords changed regularly. Appropriate staff should evaluate all apps before use, especially with regard to the security of any offsite information that may be held.

Location Services
Schools should be aware that most apps collect information as to time/date and location and this data is embedded in things such as photographs. This is not a major issue for organisations such as schools where such information is not overly personal. However staff should be aware of the technology

Security Settings On (Apple) Mobile Devices:
Obviously with pupils devices there is little value in password protecting 'low level' working with passwords
However, where staff are using devices to record information, or to create or store confidential information then there are differing levels of security that must be applied

Level 1: Apple Device own Security settings allow a Complex Alpha numeric pass-code to be set. After 10 failed login attempts, the option to ***Wipe the Device of all data*** should be activated. Age- restrictions can be set for Apps and services. Geo-location and Push notifications can be turned off.
Level2: Use Apps such as Awesome Note, Good Reader and Evernote for document Security. These all can set a **Separate Pass-code** for Opening the App when it starts.
Level 3: When in the App, pass-codes can be set to lock access to the App's internal web-browser, to its Sync folders, to the files in the App and to stop the download or syncing actions occurring by default.