

# Mobile Device Policy

## Meir Heath Academy



**Approved by**

Melanie Southern

Date: Oct 2017

**Written by**

Sheena Podmore

### **Personal mobile devices - staff**

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of devices (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Staff are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Principal and office staff aware of this, so messages can be relayed promptly.
- Staff should report any usage of mobile devices that causes them concern to the Principal.
- All staff must password protect their mobile device

### **Personal mobile devices - Visitors**

- Visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Visitors should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of devices (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Visitors are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.
- Should there be exceptional circumstances (e.g. acutely sick relative), then visitors should make the Principal and office staff aware of this so message can be relayed promptly.
- Visitors should report any usage of mobile devices that causes them concern to the Principal.
- All visitors must password protect their mobile device

### **Personal mobile devices - pupils**

- Pupils to only have phones when permission is granted from the school and parents
- Phones to be switched off during the school day
- Emergency contact to be made through the school office
- Children are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.

### **School owned mobile devices – staff**

- All mobile devices including USB sticks must be password protected to prevent data loss
- All mobile devices must be protected by the school's web filtering system
- Passwords to devices must not be shared with anyone who is not employed by the school

### **School owned mobile devices - pupils**

- All mobile devices must be protected by the school's web filtering system
- Devices intended for pupil use must not leave the school
- Pupils must access mobile devices using pupil user accounts only
- Pupil mobile device user accounts must block any attempted file downloads, block access to the computer's system files, block access to the control panel, block access to the command prompt and only map the student network drive.

**Miscellaneous**

- SSID access code to be held by the IT technician, principal, deputy head and IT Co-ordinator only.