|  |
| --- |
| **Dale Community Primary**  **and**  **Stonehill Nursery Federation**  **Mobile Technology**  **Policy** |



**Head Teacher: Louise Foster**

**Chair of Governors: Russell Langley**

**Policy Approved by: Governors Behaviour and Committee**

Policy reviewed by: Governors Behaviour and Date: 29 September 2020 Safety Committee

Policy reviewed by: Governors Behaviour and Date: 28 September 2021

Safety Committee

Policy reviewed by: Governors Behaviour and Date: 4 October 2022

Safety Committee

Policy reviewed by: Governors Behaviour and Date: 26 September 2023

Safety Committee

**MOBILE TECHNOLOGY**

**Aim**

The aim of this policy is the protection of children and adults from harm by ensuring the appropriate management and use of mobile technologies by all staff and visitors of Dale Community Primary School and Stonehill Nursery School.

Mobile technology devices may be school owned or privately owned devices that generally have the ability to connect to and utilise the school’s wireless network and Internet connectivity.

**Scope**

This policy applies to all staff members and visitors of Dale Community Primary School and Stonehill Nursery School. The purpose of this policy is to establish the correct criteria of using both school supplied devices and personal devices where the owner has established connection to the school’s network.

**Device Security**

All personal devices must adhere to a strong device policy, with a minimum of a 6-digit pin and encryption. Users must be aware of anyone using personal or shared devices when logged into school systems such as email and remote access and must ensure passwords are not saved to these devices. Users should also take care to log out of school systems as soon as work has been completed.

The user is responsible for securing their school and personal devices (physically and through the use of protection software) to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited on school devices. Users are forbidden from copying any sensitive data from remote access or any other school systems to other applications on any personal device.

**Loss, theft or compromise**

If a school issued device is lost, stolen or if it is believed to have been compromised in any way, the incident must be reported immediately to the Senior Leadership Team and the ICT Team.

The safety of personal devices that are brought in to work, are at the user’s own risk. Dale Community Primary School and Stonehill Nursery School takes no responsibility for any loss, theft or damage to personal devices in any circumstances.

**User responsibility**

Staff agree to a general code of conduct that recognises the need to protect confidential data that is stored on, or accessed using any device. This code of conduct includes, but is not limited to:

* Ensuring the adequate physical security of the device.
* Staff should not store sensitive school data on personal storage devices (e.g. USB drives, external hard drives, memory cards etc.), nor can documents be saved onto desktops – saving onto the server only.
* Ensuring the device’s security controls are not subverted via hacks, jail brakes, security software changes and/or security changes on the device.
* Reporting a lost or stolen device immediately.

**Allowances**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **School Devices** | | | **Personal Devices** | | |
|  | **Staff member’s School owned laptop** | **Laptops for class (multiple users)** | **Tablets and other school devices** | **Staff member’s personal laptop** | **Staff member’s phone or tablet** | **Visitors** |
| **Allowed in school** | Yes (connected to DCPS wireless network) | Yes  (not to be taken off site without permission) | Yes  (not to be taken off site without permission) | Yes (connection to BYOD wireless network) | Yes (connection to BYOD wireless network) | Yes (connection to BYOD wireless network)\*\*\* |
| **Server access** | Yes \* | Yes | No | Only through remote | No | No |
| **Internet access** | Yes | Yes | Yes | Yes | Yes | Yes |
| **Access to printers and external hardware** | Yes | No | No\*\*\*\* | No\*\*\*\* | No\*\*\*\* | No\*\*\*\* |
| **Recording and pictures** | Yes  (stored on server) \*\* | Yes  (stored on server) \*\* | Yes  (stored internally)\*\* | No | No | No |
| \*Through the remote server when offsite  \*\*Must check if school has consent to take children’s photographs  \*\*\*We ask you not to share this password and to forget the network after leaving the site  \*\*\*\*Printing requests to be made to the office | | | | | | |

**Personal devices agreement for staff overview**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Allowed for staff** | | **Allowed outside teaching hours** | | **Allowed for some staff** | | **Not Allowed** | |
| **Mobile devices may be bought onto school premises** | ✓ | | - | | - | | - | |
| **Mobile devices may be on the person of the user** | - | | - | | ✓\* | | - | |
| **Use of mobile phones in permitted areas** | ✓ | | - | | - | | - | |
| **Taking photos on personal mobile phones or cameras** | - | | - | | - | | ✓ | |
| **Personal browsing**  **(e.g. personal emails, Personal shopping)** | - | | ✓ | | - | | - | |
| **Use of other personal devices such as tablets or reading devices** | - | | ✓ | | - | | - | |
| **Use of school emails** | ✓ | | - | | - | | - | |
| **Use of messaging apps** | - | | ✓\*\* | | - | | - | |
| **Use of social media** | - | | ✓\*\* | | - | | - | |
| \*Leadership team, PE Team and Site managers permitted  \*\* Not while connected to BYOD wireless network | | | | | | | | |

**Mobile technology – Staff: acceptable use**

At Dale Community Primary School and Stonehill Nursery School, we recognise that mobile technology plays an important part in the lives of many adults and when used as intended, can bring substantial benefits. We acknowledge the risk that they can be used for the taking, storing and using of images inappropriately in a way that denies children’s right to dignity, privacy and respect. They also have the potential to distract staff from their work with children.

Staff members may bring mobile technology onto the school site on the understanding that the device:

* Is not used in the presence of children in school, especially during class time (unless there are exceptional circumstances).
* Is stored in a secure place that is out of sight of children and is put on silent.
* Is only to be used around school in acceptable areas during break and lunch times as well as before and after school times.
* Is not to be used as a personal point of contact during school time by relatives, friends, child’s school etc.

Staff must ensure that all potential personal contacts have the school’s landline number so that initial contact is made through the office.

If staff want their personal devices to have access to Dale Community Primary Schools and Stonehill Nursery School’s Remote Access, then they must bring their device to a member of the ICT Team to have it set up.

When off-site, staff members are allowed to have their mobile devices on their person in case of emergencies in order to contact the school, with each other or with the emergency services. In this context, phones should still not be in use to make or receive personal phone calls.

Personal technology with cameras or recording equipment should not be used in any circumstance to take photos or to record a child. However, pictures of children can be taken on school devices such as class cameras and iPads (only if authorised by parents under GDPR).

Staff must take caution not to share any form of personal information with parents outside of school.

Staff are to ensure they do not browse any inappropriate websites in school, on any device.

All school issued devices should access the school’s DCPS wireless network. Personal devices can connect to the BYOD wireless network.

**Mobile technology – Visitor: acceptable use**

Visitors may bring mobile technology on to the school site but are asked to switch their devices to silent and place them out-of-sight until they leave the building and have exited the school grounds.

Agency staff are advised to follow the ‘staff: acceptable use’ section of this policy in regards to handling both personal and school devices when working at Dale Community Primary School and Stonehill Nursery School.

All visitors are to be given the password for the BYOD wireless network on request – this password is not to be shared with anyone outside of school.

Where possible, all visitors are made aware of the mobile technology policy in advance, either through written or verbal communication.

If contractors are required to have their mobile phone to hand in order to convey live information to their line manager or head office, they will seek permission to do so in advance and will be accompanied around the site.

The use of personal devices to take photographs of the site including children or staff, is strictly prohibited unless in consultation and prior agreement with school leaders.

Parents and other family members who attend school for special events (assemblies, sports days etc.) are allowed to take photographs and record videos of their own child for personal use only. They are not to share any of this media online, nor are they allowed to live stream the event.

Visitors to school will not have access to any of the schools systems such as servers and printers.

Agency staff will use the supplied login details for school devices, which will allow access to the server in order to complete expected work left by the class teacher or another member of staff.

**Staff E-mail**

Staff are permitted access to their school email on personal devices; however, the device must adhere to a strong pin policy. As a reminder, staff should always log out of their school e-mail when handing their personal or shared device to another, in order to protect school data. Staff should also be aware:

* School e-mail communication is always monitored.
* The official school email service may be regarded as safe and secure.

Users must immediately report to the Senior Leadership Team, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threating or bullying. Staff must not respond to any such communication.

Any digital communication between pupils or their parents must be school based only and professional in tone and content. These communications should only take place through school monitored systems.

Pupils will be taught about online safety issues, such as the risks attached to emails and sharing of personal data through the curriculum.

**Monitoring and Evaluation**

The policy will be reviewed as part of the schools monitoring cycle.