Mobile Devices Policy

Policy Code:	IT3
Policy Start Date:	July 2021
Policy Review Date:	July 2024

Introduction
Throughout the Trust the welfare and wellbeing of our students and staff members is paramount.

The aim of the Mobile Devices Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice. This is achieved through establishing clear and robust acceptable mobile devices user guidelines. The Policy recognises that mobile devices are effective communication tools and sets out ways to protect against potential misuse and unnecessary cost.

The Trust is aware of the enhanced functions of many mobile devices and that these can cause concern, offering distractions and disruption to the working day, and can be susceptible to misuse – including the taking and distribution of indecent images, exploitation and bullying. As it is difficult to detect specific usage, this Policy refers to ALL mobile communication devices, including Mobile Phones, Smart Phones, Smart Watches, Tablets (including iPads), and Wi-Fi Dongles.

Definition
In this policy "mobile devices" include:

Handheld devices, tablets and smart phones, or any other devices that allow for the user to be mobile.

Scope
This Policy applies to all individuals who have access to personal and work mobile devices on site. This includes staff, volunteers, committee members, students, young people, parents, carers, visitors and contractors.

This Policy should be read in relation to the following documentation:

- Child Protection Policy/Safeguarding Policy
- Behaviour Policy
- Acceptable Uses Policy
- Photography Policy
- Code of Conduct Policy

Code of Conduct
A Code of Conduct is promoted with the aim of creating a co-operative workforce where staff work as a team, have high values and respect each other, thus creating a strong morale.

Therefore, our aim is that all staff:

- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Avoid putting themselves in a compromising situation which could be misinterpreted and lead to possible allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use of **all** mobile communication devices, especially in relation to social media.
- Are responsible for self-moderation of their own behaviours.
- Are aware of the importance of reporting concerns promptly.

Misuse refers to any activity that is non-school related or could bring the school into disrepute. It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive, therefore an agreement of trust is promoted regarding the carrying and use

of mobile phones/devices within the setting which is agreed to by all users.

Personal Devices – Staff

- Personal devices should not be used by staff when pupils are present without written/emailed prior permission from the site lead.
- With permission, staff may take a personal phone out on a school activity; however, they must be turned off and not to be used unless there is an emergency. On residential stays, a personal device/phone may be used in an appropriate location away from pupils.
- Staff are not permitted to make/receive personal calls during contact time with pupils on personal devices.
- Emergency contact should be made via the school office unless other arrangements are agreed with the site lead.
- Personal mobile phones/devices should not be used in any teaching space where pupils are present.
- Use of personal phones (including receiving/sending texts and emails) should be limited to non-contact time when no pupils are present, e.g. in office areas, staff room, and empty classrooms.
- It is also advised that staff set up security to prevent unauthorised access to functions of their personal devices.
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example, to take recordings of pupils, or sharing images.
- Legitimate recordings and photographs should be captured using school equipment such as cameras, iPads and school issued mobile phones.
- Staff who use applications on personal mobile devices (including social media) need to purchase these with their own personal ID.
- Staff must be conscious of what they post on social media and must ensure that privacy settings are up to date, rigorous and limit public distribution of content.

Mobile Phones/Devices for work-related purposes

Where a mobile phone has been issued by the Trust, it will remain the property of the Trust and can be recalled at any time and content checked. The user will be responsible for its safekeeping, proper use, condition and eventual return. During the day mobile phones/devices should be with the user at all times.

Apps must be deleted when the phone/device is returned to the Central Team (due to upgrade, end of employment or any other reason). If a mobile device is connected to a personal ID, the staff member is required to unlock the device so it can be restored to factory setting and issued to another member of staff. The user must also supply all login details that have been issued to them so that the device can be reset to factory settings.

Where a mobile phone/device has been issued by the Trust the user agrees that upon termination of employment to return the phone/device. If they do not return it, or it is returned in an unsatisfactory condition, the cost of a replacement or a proportional amount of this as decided by the Trust will be taken from final monies owing or the user will otherwise reimburse the Trust.

Photographs of students can be taken on work mobiles/devices; however, these must be stored securely and the phone/device must be locked when not in use. All such photos must be deleted from the mobile device/phone within a school term (where there are three terms in a school year).

Should there be any queries on the use of the mobile device/phone the ICT Team is available to help. If staff should leave the Trust their work-related devices must be returned to the IT staff.

Social Media on Mobile Phones/Mobile Devices

- Social media platforms will only be used in accordance with the CIT Photography and Social Media Policies.
- Teachers will not engage in activities involving social media which might bring the school into disrepute.
- Teachers will not represent their personal views as those of the school on any social media platform.
- Teachers' personal information, or pupils' personal information, will not be discussed on social media
- Authors will be accurate, fair and transparent when creating or altering online sources of information.
- Social media will not be used as a platform to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals.
- Content expressed on school social media accounts will not breach copyright, Data Protection or Freedom of Information legislation.
- Teachers will request access to the school's social media accounts from the Head Teacher or the Lead IT.
- Teachers participating in social media are expected to demonstrate the high standards of behaviour as expected within the school.
- The school's social media accounts will comply with site rules at all times, particularly with regard to the minimum age limit for use of the site.

Cloud-based Data Storage

- The school is aware that data held in remote and Cloud-based storage is still required to be protected in line with the Data Protection legislation.
- Teachers ensure that Cloud-based data is kept confidential and no data is copied, removed or adapted.

Mobile Phones/Devices – offsite, educational visits, school trips

- Mobiles/devices will be used professionally and appropriately.
- Mobile phones/devices should not be used to make general contact with parents during school trips – all relevant communications will be made via the school office.
- Mobile phones/devices may only be used to contact parents in an emergency and when the trip is outside of normal school hours e.g. residential.
- Where parents are accompanying trips, they are informed not to make contact with other parents or use their phone to take photographs of students.

Personal Mobiles/Devices – Students

The Trust recognises that mobile phones/devices are part of everyday life for many of our students and can play a role in helping students feel safe and secure. However, the Trust also recognises that they can be a distraction in school and can provide a means of bullying or intimidating others. Therefore, we have drawn up a Code of Conduct for students:

- Students are not permitted to have mobile phones/devices at school or on trips unless stated in the individual school's risk assessments. The risk assessment must be reviewed by the school's Senior Leadership Team on an annual basis. The results of this meeting must be minuted.
- In the event of parents wishing for his/her child to bring a mobile phone/device to contact the parents after school, the mobile phone/device must be handed into a staff member, then stored in the school office first thing in the morning and collected at the end of the day. (The phone is left at the owner's risk).
- Mobile phones/devices brought into school and not handed in will be confiscated and returned at the end of the day. Parents/Carers will be contacted to ensure that they

understand the rules regarding phones/devices.

Where mobile phones/devices are used in or out of school to bully or intimidate others, then the Head Teacher has the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of students when they are off the school site.'

Mobile Phones/Devices – Parents
The Trust would prefer parents not to use their mobile phones/devices while in school, but it recognises that this would be impossible to regulate. The Trust asks that parents' usage of mobile phones/devices whilst on school sites is courteous and appropriate to the school environment.

The Trust allows parents to photograph or video school events such as shows, sports day, etc, using their mobile phones/devices, but insists that parents do not publish images, for example on social networking sites, that include any children other than their own (see Photography Policy).

Lost or Stolen Mobiles/Devices
The user is responsible at all times for the security of the mobile phone/device. A PIN number should be used on the mobile/device to enable maximum security. All confidential information, for example login details, must be password protected and changed on a regular basis. If the phone/device is lost or stolen, a member of the IT staff should be informed immediately. If this is not possible then contact the provider directly, quoting the PIN number to ensure that the account is stopped and there is no unauthorised usage. In the event of a theft of a mobile phone/device, the incident must also be reported to the Police and an incident number obtained and used to report to the ICT staff.

Monitoring of Usage and Costs
The Trust's phone bills are monitored on a monthly basis and if a user's bill is over the designated monthly cost, then the user is contacted by the ICT Team. If the reason for the higher cost is work-related then no extra cost is incurred; if the calls were personal then the Trust would bill the user for anything above the designated monthly fee. Mobile phones can be spot checked at any time. Such checks will be undertaken by a member of the IT Team or Executive Leadership Team and will ensure that the phone has been used appropriately. The user will be told of the UK inclusive allowances when the phone is issued.

Mobile Phone Use Abroad
The Trust phones used abroad will be charged at cost to the user, unless the calls are required for school. Prior to the trip abroad, that user must contact the IT Department to give advice and to check the usage abroad. The user will switch off 'data roaming' unless Internet access is needed, as this may be charged at a premium rate abroad.

Policy Review
The Trust considers the Mobile Phone/Mobile Device Policy to be important and the Executive Leadership Team will undertake a thorough review of the policy and practice every three years.