Bring Your Own Device Policy

Policy Statement

The School recognises that many employees will have their own personal mobile devices (such as smartphones and tablets) which they could use for School purposes and also that there can be benefits for both the School and staff in permitting such use. However, the use of personal mobile devices for school purposes can give rise to an increased risk in terms of the security of the School's IT networks and communications systems, the protection of confidential or otherwise sensitive information and compliance with legal obligations, such as data protection requirements.

With the prior permission of their manager, employees may use a personal mobile device for school purposes, provided always that they adhere to the terms of this policy. However, employees are not required to use their personal mobile device for school purposes if they do not wish to do so.

Before using a device under this policy for the first time, employees must erase all information and software related to any previous employment.

Scope and Purpose of the Policy

This policy applies to all employees who use a personal mobile device for school purposes. It applies to use of the device both during and outside your normal working hours and whether or not your use of the device takes place at your School. This policy applies to all devices which are used to access the School's IT resources and communications systems, which may include smartphones, mobile phones, tablets, laptops etc.

When you access the School's systems, you may be able to access data about the School and our pupils, parents, contractors or suppliers, including information which is confidential or otherwise sensitive. When you access the School's systems using a device, the School is also exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to the School's systems or data), the threat of malware (such as viruses, spyware or other threats that could be introduced via a device) and the loss, wrongful disclosure or unauthorised alteration or deletion of School data (which could expose the School to the risk of non-compliance with legal obligations relating to confidentiality, data protection and privacy).

The purpose of this policy is to protect the School's systems and data and to prevent School data from being deliberately or accidentally lost, disclosed, deleted or altered, while enabling employees to access the School's systems using a device.

Connecting Devices to the School's Systems

Connectivity of all devices is managed by the JCComtech, who must approve each device as providing an appropriate level of security before it can be connected to the School's systems or network. The JCComtech has the absolute discretion to approve or reject a device and the School reserves the right to refuse or revoke permission for a particular device to connect with its systems, for example where a device is being or may be used in a way that puts, or could put, the School and its employees, pupils, parents, systems or data at risk or that may otherwise breach this policy. In order to access the School's systems, it may be necessary for the JCComtech to install software applications on the device. If any such software is removed, access to the School's systems will be disabled.

The School has the absolute right to determine what types of data can be processed on a device and what may not and you will be advised of any types of data that is restricted or prohibited.

The School's The Acceptable use of ICT policy will also continue to apply as appropriate to the device, for example where Internet sites or work e-mails are accessed on the device via the School's network.

Where a device which is connected to the School's systems develops a technical problem, fault or failure, the JCComtech will provide initial technical support to assist in determining if the issue with the device is software or hardware related. If the issue is hardware related or relates to software which you have installed, then you will be responsible for resolving it, including any repairs, maintenance or replacements costs and services. If it relates to software the School has provided, then it will provide any necessary support.

Device Monitoring

The content of the School's systems and data is the property of the School. All data, information and communications, including but not limited to e-mail, telephone conversations and voicemail recordings, instant messages and Internet and social media postings and activities, created on, transmitted to, received from, or stored or recorded on a device during the course of the School's business or on the School's behalf is the School's property, regardless of who owns the device.

The School reserves the right (remotely or otherwise) to inspect, monitor, intercept, review, disclose, remove or destroy all content on the device that has been created for or on behalf of the School and to access applications used on it for this purpose. This includes the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, printing, removal, destruction or deletion of transactions, messages, communications, posts, log-ins, recordings and other uses of the device. It is possible that

personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, employees should have no expectation of privacy in any personal data on the device. Employees are advised not to use the School's systems for communications of a sensitive or confidential nature because it is not guaranteed to be private.

The purposes for such monitoring are:

- to promote productivity and efficiency
- to ensure the security of the School's systems and their effective operation
- to prevent misuse of the device and protect School data
- to ensure there is no unauthorised use of the School's time or systems
- to ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
- to ensure that employees do not used the School's facilities or systems for any unlawful purpose or activities that may damage the School's reputation
- to ensure there is no breach of confidentiality or data protection.

The School may also store copies of any content for a period of time after it is created and may delete such copies from time to time without notice.

By agreeing to use your personal mobile device for School purposes, you confirm your agreement to such inspection or monitoring and to the School's right to copy, erase or remotely wipe the entire device, including any personal data stored on the device. Although the School does not intend to wipe personal data, it may not be possible to distinguish all such information from School data. You should therefore regularly backup any personal data contained on the device.

You also agree that you use the device at your own risk and that the School will not be responsible for any loss, damage or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of the device, its software or its functionality.

You must co-operate with the School to enable such inspection or monitoring, including providing any passwords or pin numbers necessary to access the device or relevant applications.

The School shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless absolutely necessary. If such copying occurs inadvertently, the School will delete such personal data as soon as it comes to its attention.

Security Requirements

You must:

- at all times, use your best efforts to physically secure the device against loss, theft or use by persons who have not been authorised to use the device. You must secure the device whether or not it is in use and whether or not it is your current possession. This includes passwords, encryption technologies and physical control of the device
- install any anti-virus or anti-malware software at the School's request before connecting to its systems and consent to the School's procedures to manage the device and secure its data, including providing the School with any necessary passwords
- protect the device with a pin number or strong password, and keep that pin number or password secure at all times. If the confidentiality of a pin number or password is compromised, you must change it immediately
- ensure that access to the device is denied if an incorrect pin number or password is input too many times and ensure that the device automatically locks if inactive for a period of time
- maintain the device's original operating and security system and settings, and keep it current with security patches and updates
- prohibit use of the device by anyone not authorised by the School, including family and friends
- not download and install untrusted or unverified software or applications unless explicitly authorised by the School – *JCComtech 01603 810343*
- not download or transfer any restricted or prohibited types of School data to the device, for example via e-mail attachments, or store any such restricted or prohibited types of School data on the device unless you have been specifically authorised to do so, and you must immediately erase any such information that is inadvertently downloaded to the device
- not backup the device locally or to cloud-based storage applications where that might result in the backup or storage of School data and any such backups inadvertently created must be deleted immediately
- where you are permitted to store School data on the device, ensure that it is encrypted using appropriate encryption technologies approved by the JCComtech.

If the School discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, it shall immediately remove access to its systems and, where appropriate, remove any School data from the device.

In the event of a lost or stolen device, or where you believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must report the incident to Lucy Palmer-Nortcliffe immediately. Appropriate steps will be taken to ensure that School data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all School data on the device

(including information contained in a work e-mail account, even if such e-mails are personal in nature). Although the School does not intend to wipe personal data, it may not be possible to distinguish all such information from School data.

On termination of employment, on or before your last day of employment by the School, all School data (including work e-mails), and any software applications provided by the School, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the JCComtech for wiping and software removal. You must provide all necessary co-operation and assistance to the JCComtech in relation to this process. The same process will apply if you intend to sell the device or to return it to the manufacturer or take it to a third party for repair or replacement.

Costs

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase, repair or replacement costs. You acknowledge that you are responsible for all costs associated with the device and that your School usage of the device may increase your voice and data usage charges.

Disciplinary Action

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the School's disciplinary procedure. Breach of this policy may also lead to the School revoking your access to its systems, whether through a device or otherwise.

Employees are required to co-operate with any investigation into suspected breach, which may involve providing the School with access to the device and any relevant passwords and login details.