Bring Your Own Device (BYOD)
Policy on the use of personally-owned devices

1 Introduction

About this policy

This policy is designed to regulate the use of personally-owned devices within Holmwood School ("the Employer") and to ensure that personally-owned devices are used in a manner which protects the confidentiality of company information and safeguards personal data of the Employer's data subjects.

Within the context of the use of personally-owned devices, the Employer intends for this policy to take precedence over any other company document within which reference is made to personally-owned and / or approved devices.

2 Scope and application

This policy applies to all employees and former employees of the Employer during and after the course of their employment.

For the purpose of this policy, personally-owned devices are limited to mobile phones, laptops and tablets.

3 Conditions of Use

Approved devices

All employees are required to notify their direct manager of an intention to use a personally-owned device in connection with their employment. With the approval of his or her direct manager, an employee may use a personally-owned device for purposes related to the fulfilment of his or her roles and responsibilities under the relevant contract of employment.

Where one or more personally-owned device is intended to be used by an employee, each device must be approved prior to its use for purposes related to the fulfilment of the employee's roles and responsibilities under the relevant contract of employment.

A list of approved devices will be maintained and stored within [*place of storage e.g. central database*] by [*name of department responsible for maintaining the list of devices e.g. HR*]. The list of devices will include: the name of the device user, the department of the device users, the type of device used, and its make and model.

All managers are responsible for informing [*name of responsible department*] of approved personally-owned devices within 14 days of approval.

The use of any personally-owned device for purposes related to the fulfilment of the employee's roles and responsibilities under the relevant contract of employment prior to approval is strictly prohibited.

4 Security

When using an approved device, employees guarantee that they are, at all times, the sole user of the device.

Approved devices must be password protected or secured by a biometric access control (e.g. fingerprint scanner or facial recognition). Any password applied to an approved device must be kept confidential and must not be shared with any other internal or external persons.

When not in use, approved devices must be locked to prevent any unauthorised access and must be configured to automatically lock after a maximum idle period of 5 minutes.

Approved devices should not be used in a manner which puts at risk confidential information and personal data connected to the Employer e.g. by accessing links in suspicious emails or using potentially harmful applications.

Approved devices, particularly computers are to be installed with anti-virus software throughout the duration of their use in connection with the employee's employment.

Copying of data from approved devices to other devices which are not owned by the employer is strictly prohibited.

In the event that an approved device is lost, stolen or damaged, this may constitute a security breach or a personal data breach. Upon becoming aware that the approved device may be lost, stolen or damaged, the employee must inform his or her direct manager without undue delay and no later than 24 hours after having become aware. In the case of mobile phones and tablets, the employee must immediately upon becoming aware of the loss or theft of an approved device, contact the relevant network provider to block the device.

In the event that the use of an approved device is to be discontinued or the device is to be disposed of or sold, the employee must ensure that all company-related information, confidential information and personal data processed in connection with and in the course of the employee's employment is transferred to the Employer and wiped from the approved device. The employee shall promptly inform his or her direct manager of devices no longer used in connection with the employee's employment.

In the event that the employee's contract of employment is terminated by the employee or the Employer, the employee must ensure that all company-related information, confidential information and personal data processed in connection with and in the course of the employee's employment is transferred to the employer and wiped from the approved device. The employee must remove access to any work email accounts, any data belonging to the Employer or the Employer's customers / clients and employees.

Upon the request of the Employer, the employee or former employee must provide evidence that the data referred to in the previous paragraph has been duly deleted from the device.

5 Rights of the Employer

During the course of employment, the Employer may revoke the approval of a personally-owned device. In such cases, the Employer may require the employee to use a company-owned device for the fulfilment of his or her roles and responsibilities under the relevant contract of employment.

During the course of employment, the Employer may request access to an approved device for the purpose of any investigation reasonably conducted by the Employer.

In the case of termination of employment or a change in the employee's employment which renders unnecessary the employee's access to company data stored on an approved device, the Employer may selectively wipe any company-related confidential information, personal data and access rights from the device.