Swift Academies
Employee's working remotely and Bringing Your Own devices to Work (BYOD) Policy

Accepted by: Board of Directors May 2018
Approving Body : Board of Directors
Committee : Standards
Review Cycle: 2 years
Last reviewed: June 2020
Date for next review: June 2022

1. Introduction

This policy applies to employees who work remotely or who bring their computers and/or other electronic devices, such as smartphones, mobile phones and tablets into work. This **Policy on Employees' working remotely and Bringing Your Own Devices to Work (BYOD)** is intended to protect the security and integrity of any personal data and the School's technology infrastructure. It should be read in conjunction with the Swift Academies Trust **IT Acceptable Use Policy.**

With the prior agreement of the Trust ICT Manager, all employees are permitted to use their own devices for work-related purposes. However, employees must agree to the terms and conditions set down in this policy in order to access school related content via these devices.

2. Acceptable use

The employee is expected to use his or her devices in an ethical manner at all times in accordance with the School's **IT Acceptable Use Policy and E-safety Policy.**

The School defines acceptable use of employee's own mobile devices such as phones or tablets as:

- Activities that directly or indirectly support the work of the School
- Reasonable and limited personal communication or recreation, such as reading or game playing outside of working hours

Devices' camera and/or video capabilities must be not used while on-site.

Mobile devices such as phones or tablets may not be used at school to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another School
- Harass others
- Engage in outside School activities during working hours

Employees may use their mobile device to access the following School owned resources: email, calendars and contacts.

Employees should be aware that any personal device used at work may be subject to discovery in litigation and may be used as evidence in any action against the School.

3. Remote Working

Employees who wish to work remotely outside of school can use their mobile devices to access the same information advised in Section 2 subject to the same conditions.

Employees who wish to work remotely using a PC or laptop need to refer to section 5.2 below.

4. Data Protection Act

The GDPR 2018 requires the School to process any personal data in accordance with the eight data protection principles (see the Trust's GDPR Data Protection Policy). 'Processing' includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and disposing of it. This policy applies, in particular, to the seventh data protection principle which requires the School to ensure that personal data is protected by appropriate technical and organisational measures against unauthorised or unlawful processing or disclosure and against accidental loss, damage or destruction.

5. Employees' Obligations in respect of BYOD

5.1 Security

- In order to prevent unauthorized access, devices must be password protected using a strong password or PIN
- Any device used must lock itself with a password or PIN if it is idle for five minutes
- Any device used must be capable of locking automatically if an incorrect password is entered after several attempts
- Employees must ensure that, if they transfer data, they do so via an encrypted route such as Password protected files or encrypted e-mails
- Employees must not download unverified apps that may present a threat to the security of the information held on their devices
- Employees should not use unsecured networks
- The loss or compromise of a device used for work-related activities must be reported at the earliest opportunity to the Trust ICT Manager.
- Users should log out of all remote access systems including e mail when they have finished working.
- Employees should not download or screenshot sensitive data when accessing it from a portable device.
- Employees should ensure that information displayed on the screen cannot be seen by any third party when accessing sensitive data.

5.2 Remote working, devices and procedures

- Portable devices must be presented to the Trust ICT Manager for review of software and security compliance before employees can access the network.

- The school expects users to keep their personal PC's up to date in terms of Anti-virus software if they intend to use these devices to access school data.
- Remote access to the school system will be provided through the designated software programs e.g. Remote Desktop and Office 365-One Drive which are virtual password protected environments.
- Electronic documents moved from school to remote venues must **only** be done using encrypted memory sticks or encrypted hard drives provided by the school.
- Documents containing personal data sent via e mail must be password protected (with the password being given to the person receiving the file over the phone). E mails with personal details in the body of the message must be encrypted in every instance.
- When working from home, screens are directed so that third parties cannot view sensitive data.
- Data will not be printed off site.

5.3 Retention of Personal Data

- Employees must not keep personal data for longer than necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer in order to comply with a legal obligation.

5.4 Deletion of Personal Data

- Employees must ensure that, if they delete information from a device, the information must be permanently deleted rather than left in the device's waste management system.
- If removable media, e.g. a USB drive or CD, is used to transfer personal data, employees must ensure that the personal data is deleted after the transfer is complete.

5.5 End of Employment

- Prior to the last day of employment with the School, all employees must delete work-related personal data on his/her own device(s)

5.6 Third-Party Use of Devices

- Employees must ensure that, in the event of friends or family using their devices, they are not able to access any work-related personal information by, for instance, password-protecting the information.

6. Monitoring

The School will monitor data protection compliance in general and compliance with this policy in particular. Before any monitoring is undertaken, the School will identify the specific purpose of the monitoring.

The School shall ensure that any monitoring of communications complies with the GDPR 2018.

7. Non-Compliance

Any employee found to be breaching this policy will be treated in line with the School's usual disciplinary procedure. Breaches of this policy could result in disciplinary action up to, and including, dismissal. Employees should be aware that they may incur personal criminal liability for breaches of this policy.

8. Review

This Policy on Employees' working remotely and Bringing Your Own Devices to Work (BYOD) will be reviewed every two years.