USE YOUR OWN DEVICE POLICY

Document Owner: Data Protection Officer

Date: September 2020

Status: Statutory / Non-statutory

Document Type		Use Your Own Device Policy			
Reference Number		CLT-YOD-V1.0			
Summary		The City Learning Trust (Trust) and Member Academies recognise the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, on any of our Trust sites or when travelling. Such devices include laptops, smart phones and tablets and the practice is commonly known as 'use your own device' or UYOD.			
Associated Documents		• Data Protection Policy			
Target Audience		All Staff, Governors, Trustees and Volunteers			
Document Version No:		V1.0			
Date of this Version		September 2020			
Document Owner		Data Protection Officer			
Review Body		Policy & Procedures Working Party			
Union Consultation Date/s:		n/a			
Review Body Meeting Date					
Approved/Ratified by		Board of Trustees			
Approval Date					
Date uploaded on website/s					
CLT	Haywood	Trentham	Mill Hill	Smallthorne	
Review Frequency		Bi-Annual			
Review Date:		August 2022			
Signature of Chair of Trustees					
Acknowledged by:	**Local Governing Committee:**				
	Haywood	Trentham	Mill Hill	Smallthorne	

VERSION CONTROL

Version No:	Type of change	Date	Revisions from previous version
1.0	New Document	Sept 2020	New Policy

TABLE OF CONTENTS

1. STATUS

a. Non statutory.

2. INTRODUCTION

a. The City Learning Trust (Trust) and Member Academies recognise the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, on any of our Trust sites or when travelling. Such devices include laptops, smart phones and tablets and the practice is commonly known as 'use your own device' or UYOD. The Trust is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing Trust and Member Academy services on UYOD.

b. The use of such devices to create and process Trust information and data creates issues that need to be addressed, particularly with regard to information security.

c. The Trust must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. We must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information

3. INFORMATION SECURITY POLICIES

a. All relevant Trust policies still apply to staff UYOD. Staff should note, in particular, the Trust Information Security related policies.

b. Retention Policy

c. General Data Protection Policy

d. Online Safety Policy

e. Remote Learning & Online Communication Acceptable Use Statement.

4. THE RESPONSIBILITIES OF STAFF MEMBERS

a. Individuals who make use of UYOD must take responsibility for their own device and how they use it. They must:

   i. Familiarise themselves with their device and its security features so that they can ensure the safety of Trust information (as well as their own information).

   ii. Invoke the relevant security features.

   iii. Maintain the device themselves ensuring it is regularly patched and upgraded.

   iv. Ensure that the device is not used for any purpose that would not be compliant with the Trust's Policy on the Use of ICT & equipment.

b. While City Learning Trust IT staff will always endeavour to assist colleagues wherever possible, the Trust cannot take responsibility for supporting devices it does not provide.

4.1 Staff using UYOD must take all reasonable steps to:

i. event theft and loss of data.

ii. Keep information confidential where appropriate.

iii. Maintain the integrity of data and information, including that on CLT sites

iv. Take responsibility for any software they download onto their device.

4.2 Staff using the UYOD must:

i. Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.

ii. Set up remote wipe facilities if available and implement a remote wipe if they lose their device.

iii. Encrypt documents or devices as necessary. **Staff are requested to bring their device to IT Support team members for encryption**

iv. Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices.

v. Where it is essential that information belonging to the Trust is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails.

vi. Ensure that relevant information is copied back onto Trust systems and manage any potential data integrity issues with existing information.

vii. Report the loss of any devices containing Trust data (including email) to the Data Protection Officer.

viii. Be aware of any Data Protection issues and ensure personal data is handled appropriately.

ix. Report any security breach immediately to the Data Protection Officer and ensure personal data is handled appropriately.

x. Ensure that no Trust information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party.

5. MONITORING AND ACCESS

a. The Trust will not routinely monitor personal devices. However, it does reserve the right to:

   i. Prevent access to a particular device from either the wired or wireless networks or both.

   ii. Prevent access to a particular system.

   iii. Take all necessary and appropriate steps to retrieve information owned by the Trust.

6. DATA PROTECTION AND UYOD

a. The Trust and Member Academies must process 'personal data' that is data about identifiable living individuals in accordance with Data Protection Act 2018. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

b. The Trust and Member Academies, in line with the guidance from the Information Commissioner's Office on UYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using UYOD to process personal data.

c. A breach of the Data Protection Act can lead to the Trust receiving a substantial fine. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the Trust and Member Academies facilities being withdrawn, or even criminal prosecution.

7. MONITORING AND REVIEW

a. This policy has been approved by the Board of Trustees. It will be reviewed by the Policy and Procedures Working Group on a bi-annual basis to ensure continuing compliance.