



BRING YOUR OWN DEVICE POLICY

Blackpool FC School and BFCCT

August 2018

Reviewed August 2021

1.0. Introduction

Blackpool FC School recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, in the office or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. Blackpool FC School is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing Blackpool FC School provided services on BYOD.

The use of such devices to create and process Blackpool FC School and BFCCT information and data creates issues that need to be addressed, particularly in the area of data protection and information security.

As an organisation BFCCT and Blackpool FC School 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.

2.0. Data protection policies

All relevant BFCCT and Blackpool FC School policies still apply to staff using BOYD. Staff should note, in particular, the BFCCT data protection related policies.

- Data protection policy
- Privacy policy
- Data breach policy
- GDPR communications policy

3.0. The responsibilities of staff members

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

- Familiarise themselves with their device and its security features so that they can ensure the safety of Blackpool FC School and Community Trust information
- Utilise the relevant security features (e.g. passcodes, fingerprint or facial ID)
- Maintain the device themselves ensuring it is updated and patched

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data
- Keep information confidential where appropriate
- Take responsibility for any software they download to their device

Staff using BYOD must:

- Where possible store documents on the BFCCT secure cloud to prevent data being stored on a personal device
- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device
- Set up remote wipe facilities if available and implement remote wipe if they lose the device
- Encrypt documents or devices as necessary
- Must not hold information that is sensitive, personal, confidential or of commercial value on personally owned devices.

- Where it is essential that information belonging to Blackpool FC School and BFCCT is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information included in emails.
- Ensure that any relevant information is copied back onto BFCCT cloud systems
- Report the loss of any device containing Blackpool FC School and BFCCT data to the data compliance officer
- Be aware of data protection issues and ensure personal data is handled appropriately
- Report any security breach immediately to the data compliance officer
- Ensure that no Blackpool FC School and BFCCT information is left on a device indefinitely. Particular care must be taken if a device is disposed of, transferred or sold.

4.0. Monitoring and access

BFCCT and Blackpool FC School will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either a wired or wireless network or both
- Prevent access to a particular system
- Take all necessary and appropriate steps to retrieve information owned by BFCCT and Blackpool FC School.

5.0. Data protection and BYOD

BFCCT and Blackpool FC School must process 'personal data' in accordance with the Data Protection Act 1998 and General Data Protection Regulation (GDPR). Sensitive personal data is information relating to race/ethnic origin. Religious beliefs or detailing criminal records. This category of information should be handled with a higher degree of protection at all times.

BFCCT and Blackpool FC School recognises the risks associated with using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data.

A breach of data protection under the new GDPR rules can lead to a fine of up to 4% of annual turnover. Any member of staff to have deliberately breached the Data Protection Act and GDPR may be subject to disciplinary proceedings, having access to facilities withdrawn, or even criminal prosecution.

For further information regarding BFCCT and Blackpool FC School data protection see the BFCCT Data Protection Policy.

6.0. Reviewing of the policy

This policy will be reviewed annually and when there is a data breach or serious issue raised through staff using their own devices.