Bournemouth CVS
Registered Charity No: 1081381
Company Reg'd in England & Wales No: 4024662

Registered Office
Boscombe Link,
3 - 5 Palmerston Road,
Bournemouth,
BH1 4HN
Tel & Fax: (01202) 466130
Email: contactus@bournemouthcvs.org.uk

BRING YOUR OWN DEVICE (BYOD) POLICY

1. Purpose

1.1 This policy defines acceptable use by BCVS Users whilst using **their own** devices for accessing, viewing, modifying and deleting of BCVS held data and accessing its systems. This policy applies to all Users accessing BCVS Services

2. Assumptions

2.1 Bournemouth Council for Voluntary Service ("BCVS") is a data controller, for the purposes of the Data Protection Act (1998). It is assumed that all staff have an awareness of the Data Protection Act (1998), that they will comply with the BCVS Data Protection Policy and that they understand the consequences of the loss of BCVS owned personal data.

2.2 This policy should be read in conjunction with the BCVS's policies on Data Protection, IT Security and IT & Electronic Communications.

3. Definitions

3.1 BYOD – Bring Your Own Device refers to Users using their own device (which is not owned or provided to you by BCVS) to access, but not store, BCVS information, whether at the place of work or remotely, typically connecting to the BCVS's Wireless Service.

3.2 Data Controller - The Data Controller is a person, group or organisation (in this case BCVS) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.3 User – A member of staff, volunteer, Trustee, contractor or another person authorised to access and use BCVS's systems.

4. Introduction

4.1 This policy covers the use of non-BCVS owned electronic devices to access corporate systems and BCVS information, alongside their own data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

4.2 If you wish to use BYOD to access BCVS systems, data and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided by the Data Protection Officer.

4.3 It is the BCVS's intention to place as few technical and policy restrictions as possible on BYOD subject to BCVS meeting its legal and duty of care obligations.

4.4 You may only use BOYD if the device is solely used by you, or if shared with others if you set up a separate profile with a secure password that you do not share with anyone and cannot be accessed by anyone with administration rights.

4.5 BCVS, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a User you are required to keep BCVS information and data securely. This applies to information held on your own device, as well as on BCVS systems. You are required to assist and support BCVS in carrying out its legal and operational obligations, including co-operating with the Data Protection Officer should it be necessary to access or inspect BCVS data stored on your personal device.

4.6 BCVS reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its staff, volunteers, users, business, reputation, systems or infrastructure.

4.7 Advice and guidance on all aspects of this Policy are available from the Data Protection Officer.

5. System, Device and Information Security

5.1 BCVS takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care.

5.2 The use of your own device **MUST** adhere to BCVS's IT Security and IT & Electronic Communications Policies.

5.3 In particular, when you use your own device as a work tool, you **MUST** maintain the security of BCVS's information you handle (which includes but is not limited to viewing, accessing, storing or otherwise processing).

5.4 From time to time, BCVS may require that you install or update BCVS-approved device management software on your own device.

5.5 It is your responsibility to familiarise yourself with the device sufficiently to keep data secure. In practice this means:

- Preventing theft and loss of data (using PIN/Password/Passphrase/Fingerprint lock)
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

5.6 You **MUST NEVER** retain personal data from BCVS systems on your own device without the permission of your line manager and Data Protection Officer (who will record what data is being stored). You should use your web browser to access e-mails and Dropbox and not download any data.

5.7 You **MUST**:

- use the device security features, such as a PIN, Password/Passphrase, Fingerprint, automatic lock (including if idle for 5 minutes and 5 failed login attempts), auto wipe (wipes all data after 10 failed log ins) to help protect the device when not in use.
- keep the device software up to date, for example using Windows Update or Software Update services.
- activate and use encryption services and anti-virus protection if your device features such services.
- install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.
- remove any BCVS information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them.
- do not sync any data to your device.
- remove all BCVS information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

5.8 In the event that your device is lost or stolen or its security is compromised, you **MUST** promptly report this to the Data Protection Officer, in order that they can assist you to change the password to all BCVS services (it is also recommended that you do this for any other services that have been accessed via that device, e.g. social networking sites, online banks, online shops). You must also cooperate with BCVS officers in wiping the device remotely, if BCVS deem it necessary to prevent the loss of BCVS's personal data and/or breaching of BCVS's IT security systems, even if such a wipe results in the loss of your own data, such as photos, contacts and music (it is your responsibility to back up all your own data).

5.9 You **MUST NOT** attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak'[1] the device.

5.10 Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the Data Protection Officer.

6. Monitoring of User Owned Devices

6.1 BCVS will not monitor the content of your personal devices, however BCVS reserves the right to monitor and log data traffic transferred between your device and BCVS systems, both over internal networks and entering BCVS via the Internet.

6.2 In exceptional circumstances, for instance where the only copy of a BCVS document resides on a personal device, or where BCVS requires access in order to

[1] See http://en.wikipedia.org/wiki/IOS_jailbreaking and http://en.wikipedia.org/wiki/Android_rooting

comply with its legal obligations (e.g. under the Data Protection Act 1998, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) BCVS will require access to BCVS data and information stored on your personal device. Under these circumstances all reasonable efforts will be made to ensure that BCVS does not access your private information.

6.3 Under some circumstances BCVS may then need to monitor the device at a level which may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data.

6.4 You are required to conduct work-related, online activities in line with BCVS's Data Protection, IT Security and IT & Electronic Communications Policies. This requirement applies equally to BYOD.

7. Support

7.1 Where possible the BCVS supports all devices, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy. Help and advice is available on a reasonable endeavours basis, via the Data Protection Officer, including help installing and configuring apps and other software.

7.2 BCVS takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided. Nor will it contribute to any phone/data plans, roaming charges, plan overages, etc.

8. Use of Personal Cloud Services

8.1 Personal data as defined by the Data Protection Act (1998) and BCVS confidential information may not be stored on personal cloud services[2].

9. Compliance Sanctions and Disciplinary Matters

9.1 Failure to comply with this policy may constitute grounds for action under BCVS's disciplinary policy.

Date

Signed

Chair of BCVS Board Chief Executive BCVS

Policy agreed: 1 December 2016
To be reviewed by December 2020

[2] Such as Apple iCloud, Dropbox, Google Drive, Microsoft Skydrive, etc.