BRING YOUR OWN DEVICE POLICY

FOR THE DIOCESE OF PORTSMOUTH

1 INTRODUCTION

1.1 The Diocese recognises the benefits that can be achieved by allowing staff, clergy and volunteers to use their own electronic devices when working or undertaking their ministry or volunteering tasks for the Diocese or its parishes, whether that is at home, in the Diocesan offices or on parish premises, or while travelling.

1.2 Such devices include laptops, smartphones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. The Diocese is committed to supporting staff and volunteers in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on those accessing Diocesan systems and Diocesan data using their own devices.

1.3 The use of personal devices to process Diocesan data creates issues that need to be addressed, particularly regarding information security.

1.4 The Diocese, as a data controller, must ensure that it remains in control of all data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff, clergy and volunteers to ensure that they protect their own personal information.

2 DATA PROTECTION AND BYOD

2.1 The Diocese must process personal data in accordance with the data protection laws. Special categories of personal data e.g. concerning race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation should be handled with a higher degree of protection at all times and always in accordance with the data protection laws and the Diocese's Data Protection Policy.

2.2 The Diocese, in line with guidance from the Information Commissioner's Office (ICO) on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore staff, clergy and volunteers must follow the guidance in this Policy when considering taking advantage of any authorisation given to use a personal device to access diocesan data. Authorisation must be sought from the Parish or Diocesan Data Coordinator in advance.

2.3 A data loss or breach resulting from the careless loss or misuse of your own device could result in a substantial fine for the Diocese and reputational damage.

2.4 Any member of staff found to have deliberately breached this Policy may be subject to disciplinary measures and could have access to the Diocese's facilities withdrawn.

3 THE RESPONSIBILITIES OF STAFF, CLERGY AND VOLUNTEERS

3.1 Individuals who make use of the Diocese's BYOD Policy must take responsibility for their own device, its content and how they use it. Therefore, you must:

3.1.1 familiarise yourself with your device and its security features so that you can ensure the safety of Diocesan data (as well as your own information);

3.1.2 ensure that appropriate security features and measures are in place on the device;

3.1.3 maintain the device yourself ensuring that it is regularly patched and upgraded (only using operating systems, office suites and other software which are currently supported by their suppliers); and

3.1.4 ensure that the device is not used for any purpose that would conflict with the Diocesan IT and Computer Systems Policy; in particular Section 6.18-6.25 and Section 6.49 .

3.2 While Diocesan IT staff will always endeavour to assist individuals wherever possible, the Diocese cannot take responsibility for supporting devices not provided by the Diocese.

3.3 If you are taking advantage of this Policy, you must take all reasonable steps to:

3.3.1 prevent theft and loss of Diocesan data, or the device itself;

3.3.2 keep Diocesan data confidential where appropriate;

3.3.3 maintain the integrity of Diocesan data; and

3.3.4 take responsibility for any software that you download onto the device.

3.4 If you are using your own device under this Policy, you must comply with the Diocese's Diocesan IT and Computer Systems policy and in particular Section 6.18-6.25 and Section 6.49. You must also:

3.4.1 set up pass-phrases, passwords, passcodes, passkeys or biometric equivalents (as applicable). These must be of sufficient length and complexity for the particular type of device. If your device is used to access Diocesan or parish emails, you must use a second, different password to log-in to the email account (this is called "double-locking");

3.4.2 set up remote wipe facilities (if available) and implement a remote wipe if you lose the device or allow Diocesan IT staff to do this on your behalf;

3.4.3 encrypt devices and content, as necessary;

3.4.4 not hold any information relating to Diocesan business that is sensitive, personal, confidential or of commercial value on personally-owned devices. For the sake of clarity, this means that files, images etc that relate to Diocesan business should not be kept on the C drive or other hard-drive built into the device. Instead, you should use your device to make use of storage and working services on systems that the Diocese offers or recommends, allowing access to Diocesan data securely over the internet;

3.4.5 where it is necessary for Diocesan data to be held on a personal device, delete it as soon as possible once it is no longer required. This includes information contained within emails;

3.4.6 where appropriate, ensure that Diocesan data is copied back onto the Diocesan systems, and manage any potential data integrity issues with existing information

(e.g. make sure you do not inadvertently wipe or copy over prior information or documents);

3.4.7 if Diocesan data has to remain temporarily on a device, ensure that it is backed-up daily onto a secure external medium such as an encrypted memory stick – but this should not become normal practice;

3.4.8 report the loss of any device containing Diocesan data or content to the Data Protection Officer, Mark James of MOJOU (mark@mojou.co.uk; 07443 577577) and, where possible and/or data coordinator;

3.4.9 be aware of any data protection issues and ensure that personal data is handled appropriately;

3.4.10 report any security breach immediately to the DPO, Mark James of MOJOU (mark@mojou.co.uk; 07443 577577) in accordance with the diocesan Data Protection Policy; and

3.4.11 ensure that no Diocesan data is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party to ensure that it is wiped. Ask IT support for more guidance.

4 MONITORING AND ACCESS

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

4.1.1 prevent access to a particular device from either the wired or wireless networks or both;

4.1.2 prevent access to a particular system; and

4.1.3 take all necessary and appropriate steps to retrieve Diocesan data.