DIOCESE OF LANCASTER

BRING YOUR OWN DEVICE POLICY

Diocesan Volunteers

1 INTRODUCTION

1.1 Lancaster Roman Catholic Diocese (The Diocese) relies on volunteers[1] and by the very nature of some of their roles will work from home.[2] The Diocese recognises the benefits that can be achieved by allowing volunteers to use their own electronic devices when working or undertaking their ministry within the Diocese[3] or while travelling. **nb** The Diocese has limited computer capacity in terms of mainframe and users.

1.2 In the absence of a Diocesan wide distribution of devices and an electronic system volunteers may provide their own devices. Such devices include laptops, PCs, smartphones and tablets. This list is not exhaustive. The practice of devices being provided by volunteers is commonly known as 'bring your own device' or BYOD. The Diocese is committed to supporting 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 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 and the Diocesan Data Protection Policy.

2.2 Irrespective of who owns the devices and/or systems each person is required to adhere to this policy.

2.3 All volunteers must make every effort to protect the Diocesan data from loss, unauthorised use, erasure or partial erasure, corruption and theft.

2.4 Similarly, all devices must be afforded the same protection.

2.5 A data loss or breach resulting from the careless loss or misuse of their own device by a volunteer will be reported to the Information Commissioner's Office which could result in the Diocese receiving a substantial fine and reputational damage.

2.6 Any volunteer found to have deliberately breached this policy may be subject to sanctions being placed upon them.

---

[1] Volunteer: any lay person or Religious who is not an official or employee of the Diocese

[2] This could involve using a device in the home or office of another volunteer eg Parish Safeguarding Rep.

[3] Diocese includes parishes

3 THE RESPONSIBILITIES OF VOLUNTEERS

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

3.1.1 familiarise themself with their device and its security features.

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

3.1.3 ensure that the device is not used for any purpose that would conflict with the Diocesan.

3.2 If the volunteer is taking advantage of this Policy, the individual must:

3.2.1 Take responsibility for the downloading of any software onto their device.

3.3 If a volunteer is using their own device under this Policy, the individual must comply with the Diocese's Acceptable Use Policy. The individual must also:

3.3.1 Where technically possible use a second, different password to log-in to the email account if their device is used to access Diocesan or parish emails.

3.3.2 set up remote wipe facilities (if available) and implement a remote wipe if the individual loses their device or allow Diocesan IT staff to do this on their behalf;

3.3.3 use separate and encrypted devices.

3.3.4 not hold any information relating to Diocesan business that is sensitive, personal, confidential or of commercial value on personally-owned devices.

3.3.5 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;

3.3.6 report the loss of any device containing Diocesan data or content or security breach to the Data Protection Officer

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

3.3.8 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.

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.