Print security strategy

This document provides an explanation and response to an e-mail letter which was distributed on 20 June 2017 by Kyocera document solutions. The document warns users of industrial level printers and photocopiers that it is necessary to have a security strategy in place in view of General Data Protection Regulation (GDPR) requirements .

So what's GDPR all about?

The General Data Protection Regulation comes into force on 25 May 2018 and is an attempt by the European Parliament to strengthen and unify data protection regulation within the EU and beyond. GDPR defines much harsher penalties for data protection breaches than those which currently exist, especially in the corporate arena.

Since this issue has been raised by Kyocera, our printer supplier, this document addresses actions which we might need to take only in respect of our use of a printer/photocopier. We should review all our use and management of personal data to ensure compliance with the new act when we have more information.

What has GDPR to do with printing?

Firstly, we will discuss the general issue, before we move, in the next section to local application, based upon the printing hardware which is currently implemented in the Church office.

All high-volume printers have some form of temporary memory where print requests are stored, prior to printing actually occurring. Most printers include a high-capacity hard-drive for this purpose. This offers advantages including:

1. Multiple copies of the same document need to be sent to the printer only once. This is stored once on the hard-drive and as many copies as necessary are printed from there. This is termed ‘spooling’.
2. This means that printing occurs independently of the computer which sent the document to be printed. This immediately frees up the computer to continue with further work.
3. In the event of a fault occurring, such as a paper jam, the data are not lost and the printer can recover the document from its hard-drive and continue to print the correct number of copies.

A hard-drive deployed in a printer in this manner will, of necessity be of fairly high capacity, meaning that it will probably hold a history of many recent print jobs. As the drive runs out of space, old jobs will be deleted to make space for new documents. Since it is possible that some of the many documents held on the hard drive may contain sensitive data (such as names and associated addresses or phone numbers), the need to keep them safe falls under the General Data Protection Regulations.

Such data, stored on a hard-drive, are at risk of loss through, for example:

1. Hacking into the printer via its connection to a local area network.
2. Hacking into the printer via its connection to a gateway to the Internet.
3. Hacking into the printer via a Wi-Fi connection.
4. Physical theft (of the printer, or its internal components).

How does this affect us?

Fortunately, the current church printer implementation makes many of the above concerns irrelevant.

1. The printer does not contain a hard drive, but instead a random access memory (RAM) disk. This functions as a virtual hard disk, but is a volatile form of memory; meaning that all data stored there are lost when the power to the printer is turned off.
2. The printer is not connected to a local area network, nor directly to the Internet.
3. The printer is not connected to a Wi-Fi router.
4. Physical theft of the printer would, of necessity, erase all the data on the RAM disk, because it would be disconnected from the power supply.

Are there actions which we need to take?

Although there is clearly a high level of trust within the Church, we need to consider all potential risks to data stored on the Church printer in order to satisfy data protection requirements, in the event that we be audited.

Theoretically, the printer in the church office could be hacked via the (currently unused) ethernet connection at the back of the printer. This could only happen if the printer had been left switched on and the deed was enacted by somebody with access to the office and with the necessary technical know-how.

I suggest that we take the following two actions. These should be done immediately in order to protect the Church under **existing** data protection legislation.

1. Document the necessity for the printer to be switched off ***whenever*** it is left unattended and post a clear notice in the church office to this effect.
2. Ensure that an always-current list exists of those in possession of a key giving access to the Church Office. Require that these keys be signed for.

Tony J Salt
6 July 2017