**Parish Financial Management 12. ICT**

[12.1 PARISH COMPUTER CODE OF PRACTICE](https://inside.rcdow.org.uk/parish-fin-mgmt/ict-pam/ccp/)

PLEASE PRINT, SIGN, DATE AND RETURN TO YOUR PARISH PRIEST (PP)

**THIS COMPLETED FORM MUST BE KEPT IN A FOLDER MARKED ‘GDPR COMPLIANCE’ AND MADE AVAILABLE FOR AUDIT PURPOSES**

**General overview**

Computer equipment such as PCs, networks, on-line accounts including Internet and email services, are provided by the parish to assist you with your day-to-day duties for the purpose of church business.

All computer users are advised that the ICT Department will, from time to time, monitor systems activity on the Diocesan network and internet. The Diocese will refrain from excessive monitoring of activity, but will conduct reviews of the content of messages and files, including random reviews, when in the exercise of its judgement it determines that it would be prudent to do so.

If you have specific questions regarding the diocesan policies with respect to its PCs, computer networks, or on-line accounts, please do not hesitate to contact the Diocesan ICT Department on 020 7798 9164 (x 2164).

**Care of ICT equipment**

All equipment is insured against theft and loss; however, it is the responsibility of individuals to ensure that any equipment they are issued by the parish is not damaged, lost or stolen.

Any malfunction (software or hardware) must be reported to the ICT department and not allowed to be repaired by any unauthorised third parties. Allowing unauthorised third parties to repair faulty equipment may be a breach under Data Protection and may result in disciplinary action. The action of having an unauthorised third party repair a faulty computer must be reported to the ICT Department and the Data Protection Officer immediately.

Login details and passwords must not be divulged to unauthorised users or on notes attached to the computer.

**Computer access**

All parish computer users must be authorised by the PP. For security reasons, passwords and screensaver passwords may only be issued by the PP and made known to the authorised user(s) only. Any suspected misuse of a computer by an unauthorised person should be reported to the PP immediately.

**Email**

All parishes, staff, clergy and elected volunteers must use their diocesan email accounts for business purposes. If you have not as yet been allocated a diocesan account, or cannot remember how to access your account, please contact the ICT Department who will be happy to provide assistance.

Each diocesan employee, clergy and elected volunteers, will have an email address issued by the Diocese. Any other email addresses accessible on the parish computer must be authorised by the PP.

* **Sending Personal Data**

Firstly, consider whether you should be sending personal data via email. If you have to, then create a password-protected document and send that as an attachment. Share the password separately with the intended recipient.

Delete any document, which may have been automatically downloaded into your ‘DOWNLOADS’ folder. Please do not keep Diocesan personal data stored on your devices.

**Working Away from the Parish**

With express permission of your parish priest, in your capacity as a parish volunteer, you may take materials away from the parish to be worked on, subject to the following:

1) You inform the Parish Priest what materials you are taking with you

2) When you will be returning those materials back to the parish

3) You must take care of the materials and guard them against theft or loss as these may contain personal or sensitive data

4) The materials that you take are stored safely when you are not working with them

5) If you are using your own electronic equipment, you must not download any content onto your devices

6) Any documents/spreadsheets relating to the materials from the parish and is on your electronic device remains the property of the Parish and must be deleted when you have completed the task you are undertaking

7) Any electronic data that you create off-site must be subject to password protection, for example, creating a spreadsheet of names and addresses from paper documents

**Internet policy**

Parishes must always be in a position to block inappropriate websites.

Parishes should be using the Diocesan recommended anti-virus application which will enable this to happen. Contact the ICT Department to receive this FREE of charge.

The following types of sites will be restricted:

* adult/sexually explicit
* gambling
* violence
* drugs and alcohol
* hacking
* remote proxies
* chat
* personals and dating

The best way to preserve privacy for your own personal data is to not store it on diocesan/parish computer equipment or transmit it over the Diocesan network and internet or on-line accounts.

Specifically, any personal use of the parish computers, computer networks, and on-line accounts must not:

* Interfere with the performance of your job duties (reasonable efforts should be made to limit personal use to non-business hours).
* Further, the conduct of any business other than the Church’s business, including any personal commercial ventures or private charitable solicitations
* Violate the PP’s instructions, if any.

Although the Diocese will permit the limited personal use described above, the Diocese assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted or stored using its computers, computer networks, or on-line accounts. Moreover, the Diocese accepts no responsibility or liability for the loss or non-delivery of any personal e-mail communication.

**Acceptable use of computer equipment**

It is the responsibility of staff, clergy and elected volunteers to ensure that all work equipment is used for the purpose for which it was supplied and that all current legislation in UK and EU law is adhered to. This means that any software installed on a computer system must be entirely legal – evaluation versions of software are permitted but at the end of the evaluation period it must be licensed or removed from the system.

Under no circumstances may material that is or may be construed as being pornographic, inciting racial hatred or offensive to any group in respect of their ethnic, religious or sexual orientation be stored or transmitted using diocesan equipment or Diocesan email accounts. Any violations of these rules should be immediately referred to the ICT Department initially. The ICT Department will then refer the violation to the HR Department, who may instigate the Diocesan Disciplinary Procedure.

I have read the Computer Code of Practice and agree its terms and conditions accordingly.

Signed ………………………………………………………………

Date ………………………………………

**Please give the signed and dated copy to your Parish Priest and keep a copy for yourself**