Roman Catholic Archdiocese of Southwark CIO

Computer Usage Policy

May 2018

COMPUTER USAGE POLICY FOR THE ROMAN CATHOLIC ARCHDIOCESE OF SOUTHWARK (THE "DIOCESE")

1 ABOUT THIS POLICY

1.1 This policy is designed to detail how computer systems within the Diocese must be used. It covers anyone (clergy, employees, volunteers, workers, etc.) who has access to Diocesan computer systems. Failure to adhere to this policy will be treated extremely seriously and could, in the case of employees, lead to disciplinary action.

2 PERSONNEL RESPONSIBLE FOR THE POLICY

2.1 This policy has been written by the diocesan Finance Office. It will be updated from time to time or as legislation changes. At a local level the parish priest or agency head has responsibility for ensuring that the policy is properly implemented and adhered to.

3 EQUIPMENT SECURITY AND PASSWORDS

3.1 All systems MUST be password protected. Each user of the system MUST have their own password and passwords must never be shared. You may be required to have different passwords for access to different accounts. Passwords MUST be strong and contain at least 8 characters and be a mix of upper and lower letters, numbers and characters. Passwords MUST be changed once a month.

3.2 Please remember that the data held on diocesan devices is the responsibility of the data controller and access cannot be denied to the Diocese, by the usual user. Failure to provide access if requested will lead to disciplinary action and possibly legal action.

3.3 A central repository of passwords will be retained by ICT Support in case a device needs to be accessed, for example due to absence of the user or corruption of the data.

3.4 Personal diocesan data MUST NOT be held on personally owned devices (PC, laptop, mobile phone, etc). Personally, owned devices can be used as a portal to access personal data held, for example, in the cloud, but it MUST NOT be stored on the device. If the action of accessing documents via the cloud automatically downloads them to the device, they MUST BE deleted from the device. If your personal device automatically downloads or syncs diocesan emails, this function MUST be disabled. Personal devices can be used to access diocesan emails provided that it is done via a portal. If you have personal data stored on your own device and that device is lost or stolen it would constitute a breach under the GDPR.

3.5 If you have a diocesan mobile device, it MUST be encrypted to current (May 2018) standards. Please contact ICTSUPPORT@finance-rcdsouthwark.org to check any devices you may have.

3.6 Parish/agency desktops will also need to have current encryption. Please contact ICTSUPPORT@finance-rcdsouthwark.org or visit our website to ensure that you have the most up-to-date encryption.

3.7 All parish/agency devices MUST have the most up-to-date antivirus software. Please contact ICTSUPPORT@finance-rcdsouthwark.org or visit our website to ensure that you have the most up-to-date version.

4 SYSTEMS AND DATA SECURITY

4.1 Threats to cyber security are rife and it is the most commonly exploited area for crime such as ID thefts and banking/payment fraud. Criminal access to data is achieved in a variety of ways including fake emails, emails or attachments containing viruses and users being tricked into revealing data. This means that we all have to be extra vigilant in how we manage our IT activity. NEVER open an email or attachment that looks suspicious or click on a link that you don't know what it is. Suspicious emails might be identified by unusual formatting/fonts or strange wording in the subject line or sender. Please delete any such emails without opening them. Only open attachments or click on links if you know where they have come from.

4.2 The Diocese has the right to block certain content and/or access to certain websites and users should not attempt to access blocked content or password protected areas.

4.3 You MUST NEVER load software on to Diocesan systems without the express permission of ICT Support.

4.4 If you think you may have accidentally introduced a virus into a diocesan system, please contact ICT Support immediately.

4.5 All systems should be regularly backed up. It is recommended that each parish/agency backs up their own system daily to an encrypted (to current standards) external drive, which is then stored in a safe. If you need help with this, please contact ICTsupport@finance-rcdsouthwark.org.

5 EMAIL

5.1 Our email code of conduct has been put in place to ensure the appropriate use of the system. The code covers all diocesan email users in the following circumstances: -

5.1.1 E-mail technology used on behalf of the Diocese, its parishes and agencies and any other associated organisations

5.1.2 E-mail technology used on hardware and/or software provided by the Diocese its parishes and agencies and any other associated organisations

5.1.3 The technology used to communicate information about the Diocese and associated organisations and people

5.1.4 The technology used to communicate any information that has been gained from the Diocese its parishes and agencies and any other associated organisations

5.1.5 The email system provided by the Diocese is for Diocesan business use and can be accessed by the Diocese. If you use it for personal use you do so at your own risk and accept that those emails are also accessible by the Diocese. If you do not wish any personal emails to be accessed DO NOT use your Diocesan email address for personal use.

The rules of the Code are as follows: -

5.2 Bullying, harassment or abuse of others through the use of email is forbidden. This includes sending information that insults or harasses others with respect to gender/gender reassignment, religion/belief, ethnic/national origin, age, sexual orientation, martial/civil partnership status, pregnancy/maternity or disability. If anyone feels that they have been bullied or harassed via email, please raise your concerns with the HR Manager in the first instance.

5.3 It is expressly forbidden to: -

- Access or distribute illegal images
- Access or distribute pornography
- Engage in on line gambling
- Take part in electronic chain letters or other types of messaging
- Send or forward junk email
- Run a business
- Download or distribute copyright information
- Download, open or distribute unauthorised software
- Post confidential information about the Diocese or any related parties without authorisation.
- Send data belonging to the Diocese to a home computer or other personal device

5.4 When replying to an email, make sure that the reply is for the sender only and not original mailing list (unless there is a requirement to do so).

5.5 When attaching files to a message, keep them small and ensure that they are PASSWORD PROTECTED if they contain personal data. Email is not the medium to use for very high resolution graphics. In addition, do not attach files that have hidden confidential information. Software exists that can reveal this hidden data.

5.6 Remember: -

- Emails can be read by third parties (police can obtain printouts directly from internet service providers without a warrant).
- Email can be used in evidence.
- Email can create binding contracts.
- Email may contain content which is subject to the Data Protection Act
- Make sure that the content of your email is factually correct and non-defamatory.
- Emails have to be disclosed in certain legal proceedings

5.7 It is forbidden to send email using a mail client (i.e. software) that has been installed for another employee (i.e. someone else will appear to be the sender.). In addition, employees must take adequate precautions to prevent this (e.g. ensure that PC's are not left switched on and unattended for long periods of time).

5.8 An individual's PC may be audited at any time to ensure compliance to the code of conduct.

5.9 Please ensure your Email has the approved **Diocesan Signature and Disclaimer** at the bottom of all sent Emails. The current wording is:

Name
Role Title
Parish/Agency Name and Address
Parish/Agency Telephone Number

This message is only for the use of the intended recipient(s). It may contain information which is confidential and legally privileged within the meaning of applicable law. If you are not the intended recipient, please contact the sender as soon as possible. Any copying, disclosure, distribution or any action taken or omitted to be taken in reliance on it is prohibited and may be unlawful. Unless stated to the contrary, any opinions expressed in this message are personal and may not be attributed to the Roman Catholic Archdiocese of Southwark.

6 USING THE INTERNET

6.1 The Diocese has a Social Media Policy which MUST be observed at all times. The policy is available on the diocesan website

http://www.rcsouthwark.co.uk/media/Social%20Media%20Policy%20-%20Approved%20version%20-%2017%20M11.pdf

6.2 Access to the Internet is provided for business use. **Reasonable personal use is permitted, but this must not be abused. Abuse of the system will lead to disciplinary action and may result in access to the Internet being denied to all users. It may also be reported to the police.**

6.3 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 for personal use. Moreover, the Diocese accepts no responsibility or liability for the loss or non-delivery of any personal e-mail communication.

6.4 Access to social networking sites – e.g. Facebook, Twitter, LinkedIn, etc. is not generally required as part of the business of the Diocese. Where it is part of Diocesan business – e.g. a parish Facebook page, only the diocesan social media account should be accessed through diocesan devices. Networking sites MUST NOT be left open whilst other work is undertaken as constant feeds are distracting and may permit unauthorised access.

6.5 The creation, generation and distribution of material through social media that is offensive on the grounds of gender/gender reassignment, religion/belief, ethnic/national origin, age, sexual orientation, martial/civil partnership status, pregnancy/maternity or disability is forbidden. Please remember that under current legislation complaints can be made by anyone who finds the material offensive whether or not it was directed at them personally.

6.6 It is forbidden to use the internet to generate and/or distribute material which is offensive to, or ridicules other employees or anyone else associated with the Diocese.

6.7 The use of Diocesan technology to access, store or distribute of any kind of offensive material (including all pornography) is expressly forbidden. It may also be illegal and lead to prosecutions of both the employee and the Diocese.

6.8 Any illegal activity will be reported to the police.

6.9 In these rules, material will be considered offensive if it causes distress to the person who receives it, discovers it and/or if it is defined as illegal under current legislation. Please remember that under current legislation complaints can be made by anyone who finds the material offensive whether or not it was directed at them personally.

6.10 Accidental sending or receiving of such material will not be an acceptable excuse.

6.11 The Diocese considers any breach of these rules to be serious and will automatically invoke the Disciplinary Procedure. Depending upon the nature of the breach, it could be considered as Gross Misconduct and/or involve reporting to the Police. The Diocese reserves the right to use monitoring software as it sees fit.

6.12 The following websites are specifically excluded from access at the Diocese:

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

6.13 Parishes/agencies MUST be in a position to block such websites. They should be using the Diocesan recommended anti-virus application which will enable this to happen. Contact the ICTsupport@finance-rcdsouthwark.org for more information.

7 MONITORING

7.1 Like most organisations, the Diocese has the technical capability to monitor activity on its systems and reserves the right to do so. This will not be used on a regular basis but will only be used in exceptional circumstances and/or to retrieve any lost data/history.

8 PROHIBITED USE OF OUR SYSTEMS

8.1 The Diocese takes the misuse of its systems very seriously. Failure to comply with this policy will lead to disciplinary action, which could include dismissal and may result in the involvement of the police. If banned activity is discovered remote technical steps will be taken to secure evidence and prevent further misuse.

9 WORKING AWAY FROM THE PARISH

9.1 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:

- You inform the Parish Priest what materials you are taking with you
- When you will be returning those materials back to the parish
- You must take care of the materials and guard them against theft or loss as these may contain personal or sensitive data
- The materials that you take are stored safely when you are not working with them
- If you are using your own electronic equipment, you must not download any content onto your devices
- 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
- 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

---

10 APPROVALS

This policy was approved by the Diocesan Trustees on: 24/05/2018

The next review is due on or before: 01/11/2018