IT POLICY

INTRODUCTION

The purpose of this policy is to define the duties and responsibilities of Revelation Church London (RCL) employees, including contractors and temporary staff, when using the Charity's IT, internet and email facilities, provided to assist with day to day work. It is important that employees etc. understand the legal, professional and ethical obligations that apply to them, and use these facilities responsibly.

RESPONSIBILITIES AND AUTHORISATION

All Users are expected to act in a way that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported to your Line Manager as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

No person can use the Charity's IT, internet and email facilities without authorisation by the Strategy and Operations Manager. Unauthorised access to internet and email facilities may result in disciplinary action or criminal proceedings.

SCOPE

This policy covers the following areas:

1. Legislation
2. Systems and Infrastructure
3. Hardware Provision
4. Security and Backup
5. Email Use
6. Internet Use
7. Social Media
8. Legitimate Access
9. Health & Safety
10. Policy Enforcement and Monitoring
11. Disciplinary Action

OWNERSHIP / CONTACT

The overall owner of this policy is the Strategy and Operations Manager. Please contact Andy Crawley (andy@revelationchurch.org.uk) with any questions or queries unless another person is specifically designated within the policy. If a specific person outlined in this policy is unavailable then please contact the policy owner.

LEGISLATION

All users must comply with the relevant legislation, which includes:

1. *Data Protection Act 1998/ Freedom of Information Act 2000* - Any information which the Charity holds, including emails, is potentially disclosable to a requester under one of these acts. When users write and send emails, they must ensure data protection is not breached, which could include (but is not limited to):
    - Passing on personal information about an individual or third party without their consent.
    - Holding personal information longer than necessary.
    - Sending personal information to a country outside the EEA.

Under the Data Protection Act 1998, any email containing personal information about an individual may be liable to disclosure to that individual, this includes comments, opinions, and factual information. Therefore, employees should consider this when writing and retaining emails, and, where possible, should avoid transmitting personal data about a third party.

2. *Computer Misuse Act 1990* - This Act makes it an offence to try and access any computer system without authorisation.

3. *Copyright Design and Patents Act 1988* - it is an offence under this Act to copy software without the permission of the owner of the copyright.

4. *Defamation Act 1996* - Under this Act it is an offence to publish untrue statements which adversely affect the reputation of a person or group of persons.

5. *Terrorism Act 2006* - This Act makes it a criminal offence to encourage terrorism and/ or disseminate terrorist publications.

6. *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000* - This allows an organisation to monitor or record communications, including telephone, internet, email, and fax, for defined business-related purposes.

SYSTEMS AND INFRASTRUCTURE

Due to its agile nature, the majority of RCL Systems and Infrastructure are based in a 'cloud' environment.

The key systems / software used and their purpose are outlined below. This list represents the main systems, however other systems are used from time to time to collaborate with other parties.

- **Microsoft 365** – Provides access to suite of office software, main collaboration and record keeping environment for RCL Activity (through SharePoint)
- **Google Suite** – Facilitates RCL email (incl lead@relationalmission.com address)
- **Revelation Church Website** – Hosts and facilitates RCL's web presence (hosted / facilitated by Wix)
- **1-2-3 Reg** – Domain host
- **Xero** – Bookkeeping and accounting system for RCL
- **Backupmybooks** – Cloud backup for accounting records on Xero
- **ChurchSuite** – church / contact database for RCL, used to facilitate Church Groups, events, ministries and giving records / Gift Aid
- **Justgiving** – Facilitates online giving facility
- **CAF** – Facilitates online giving facility
- **Stripe** – Facilitates online event and ChurchSuite bank transfer / card transactions
- **GoCardless** – Facilitates ChurchSuite direct debit payment transactions
- **iZettle** – Processing physical card payments
- **SumUp** - Processing physical card and contactless payments
- **CCLI / CCLI SongSelect** – Licencing, charts and records for worship music used by RCL
- **YouTube** –hosting RCL videos and Live Streaming, plus unlisted ID teaching videos
- **Vimeo** – hosting password protected RCL videos and LEAD training videos
- **Facebook** – RCL Social Media presence
- **Twitter** – RCL Social Media presence
- **PayPal** – processing RM Training Teachable payments
- **Instagram** – RCL Social Media presence
- **Zoom / Skype / Hangouts / MS Teams / Whats App Messenger** – Team Communications
- **Adobe Creative Cloud** – Media, graphic and design production
- **Mailchimp** – Promotion, publicity, newsletters

- **HP Instant Ink** – Office printing and cloud printing
- **Thirtyone:Eight** – processing DBS checks
- **Dataplan** – payroll provider with management portal
- **ePayslips** – payslip provider and portal for staff payslips
- **People Pension** – online pension portal
- **Podcast Generator** – management of Podcast
- **Spotify** – RCL music playlists and podcast feed
- **Apple Podcasts** – podcast feed
- **Charity Digital Exchange** – licence provider for IT systems and software
- **ID Website** –ID Training course online presence (hosted WordPress, facilitated by Business Equip)
- **Teachable** – LEAD teaching platform
- **Solid Rock Portal** – management of Newday bookings and data
- **Zipcar business portal** – transport solutions and Foodbank stock deliveries
- **Vmix** – licencing for streaming and audio solutions for Sunday services
- **Virgin Business** – broadband provider for office environment
- **Trussell Trust Foodbank Data System** – processing Foodbank voucher and donation information
- **Trussell Trust Assemble System** – management portal for managing Foodbank staff and volunteers

At the Revelation Church Office, physical IT such as printers, routers and monitors are managed and maintained by the Church Administrator, with PAT testing completed annually on such devices.

Employees, volunteers, and contractors are authorised to access this software/infrastructure, as the need requires, by the owner of this policy. All individuals accessing the RCL infrastructure will have unique individual access details. RCL covers the associated cost of this unless otherwise agreed.

HARDWARE PROVISION

RCL sets aside a financial provision each year to make sure appropriate equipment / devices (laptops, mobile devices, monitors etc) can be purchased to help its employees and volunteers in achieving the goals of the charity.

RCL will provide the appropriate equipment / devices based on the role and task that is required, at the discretion of the owner of this policy. These devices should not be used for personal use unless authorised by the owner of this policy as consideration needs to be given to the HMRC benefit / income tax regulations.

Employees and volunteers may choose to decide to use their own equipment / devices if they prefer at their own cost providing they meet the minimum requirements for the task / role and requirements outlined in the following security section. RCL may contribute to the cost of this equipment depending on how much it is directly used for the benefit of RCL and in line with HMRC benefit / tax regulations. This is at the discretion of the owner of this policy.

SECURITY AND BACKUP

With the development of technology over recent years, security and backup of information and systems has become increasingly complex, especially with the desire to access software and systems from a range of personal devices.

Below are the requirements with regard to security and backup and accessing the RCL infrastructure. This is relevant for employees, volunteers and contractors.

- While the infrastructure outlined can be accessed by RCL owned devices or personal devices, condition of access is based on a number of measures being in place or followed.

- **It is the individual user's responsibility to make sure these requirements are adhered to at all times**. If these measures cannot be put in place then access will be withdrawn.
- The requirements are:
    - Up-to-date anti-virus protection is installed on the device and firewall enabled (regularly updated).
    - A logon or passcode to the device is in place (with an auto lock in place if the device is not used for a period).
    - Device logon or passcode is not shared by anyone else.
    - If in a public place the device is not left unattended.
    - Where access has been given, documents must be saved to SharePoint or saved in the users OneDrive. This will ensure data is regularly backed up to the cloud and safeguarded.
    - If any device is stolen or has had unauthorised access then the owner of this policy must be contacted immediately (see contact details in the first section of this policy).
    - Security updates to devices should be implemented as soon as they are available.
    - Unique log on details (username/passwords) given to access specific aspects of the infrastructure must not be shared with anyone.
    - RCL's 'Confidentiality policy' and 'Data Protection Policy' which link into this policy in terms of the data / information is adhered to.
    - To follow the other provisions outlined in this policy.

All primary software systems outlined in section 1 are regularly backed up by the providers of these services (as per their terms & conditions). This is part of the criteria for selecting these systems. The LEAD training course has a number of large video files (teaching and training) that are backed up and stored securely on external hard drives by the LEAD team.

Some of these services, i.e. Xero are also backed up by third party software (Backupmybooks).

USE OF EMAIL

Emails sent or received on the email system form part of the official records of the Charity; they are not private property. It applies to use of RCL email on any device, no matter whether owned by RCL or an employee, volunteer or contractor. The Charity does not recognise any right of employees to impose restrictions on disclosure of emails within the Charity. Emails may be disclosed under the Freedom of Information Act, as part of legal proceedings (e.g. tribunals), and as part of disciplinary proceedings. Users are responsible for all actions relating to their email account/ PC username, and should therefore make every effort to ensure no other person has access to their account.

When using Charity email, users must:

- ensure they do not disrupt the Charity's wider IT systems, or cause an increase for significant resource demand in storage, capacity, speed or system performance, e.g. by sending large attachment to a large number of internal recipients.
- ensure they do not harm the Charity's reputation, bring it into disrepute, incur liability on the part of the Charity, or adversely impact on its image.
- not seek to gain access to restricted areas of the network, and other "hacking activities" are strictly forbidden.
- must not use email for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees who receive emails with this content from other employees of the Charity should report the matter to their line manager.
- not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous, or contain illegal or offensive material, or foul language.

- not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- not engage in any activity that is likely to:
    - Corrupt or destroy other users' data, or disrupt the work of other users;
    - Waste staff effort or Charity resources, or engage in activities that serve to deny service to other users;
    - Be outside of the scope of normal work-related duties – for example, unauthorised selling/ advertising of goods and services;
    - Affect or have the potential to affect the performance of damage or overload the Charity system, network, and/ or external communications in any way;
    - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights. Users must not use RCL email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
    - not send chain letters or joke emails from a Charity account. Staff who receive an improper email from individuals inside or outside the Charity, should discuss the matter in the first instance with their line manager.
- not send bulk emails using the standard business email system unless agreed
- use standard RCL email signature and any associated email disclaimer. Users must not remove or change this when they send messages.

Personal Use of Email

Personal use of the Charity email is not permitted. Users may access their own personal email accounts at work, if they can do so via RCL's internet connection. For instance, a staff member may check their Google Mail during their lunch break. Personal email use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch. All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.

Contracts and liability on email

Users must be careful about making commitments or agreeing to purchases via email. An email message may form a legally-binding contract between RCL and the recipient – even if the user has not obtained proper authorisation within RCL.

Best practice when using email

1. Employees should name an alternative member of staff for correspondents to contact if necessary, when activating the "out of office" facility messages. This will ensure that any important messages are picked up and dealt with within a reasonable timescale.

2. An employee (or manager) should make arrangements for notification, and access by another appropriate member of staff during periods of absence, when highly important emails are anticipated. Speak to the policy owner for how to manage this.

3. Employees are reminded that emails can easily be forwarded or archived without the original sender's knowledge, and may even be read by persons other than those they are intended for. Therefore, where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication.

4. Users must exercise due care when writing emails to avoid being rude or unnecessarily terse, particularly as emails sent from the Charity may be interpreted by others as Charity statements. Users are responsible for ensuring that their content and tone is appropriate, and whether it requires a formal and business-like manner, usually associated with other forms of written correspondence.

5. Users should delete all unsolicited junk mail. In the process of archiving emails, users should ensure inappropriate material is not archived.

6. Caution should be used when opening any attachments or emails from unknown sources. Furthermore, files should be downloaded from reliable sources, to the best of the employee's knowledge. It is a disciplinary offence to disable the virus software on your laptop or PC. Any concerns about external emails, including files containing attachments, should be discussed with your Line Manager

7. Users should use the BCC function when sending emails to large groups. It could be considered a breach of GDPR regulations unless every recipient has consented that their email address is available in the public domain

8. Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.

9. Only use the 'important message' setting sparingly, for messages that really are important.

Internal Email

Email is a valid way to communicate with colleagues. However, it tends to be overused for internal communication. Microsoft Teams and Office 365 should be used as the primary source of collaboration over projects/events etc.

Users should keep these points in mind when emailing colleagues also:

- Would the issue be better addressed via a face-to-face discussion or telephone call?
- Is email the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions (is using SharePoint with track changes a better option).
- It's rarely necessary to 'reply all'. Usually, it's better to reply and then manually add other people who need to see a message.

USE OF THE INTERNET

Use of the Internet by employees is encouraged where such use is consistent with their work and the goals, and the objectives of the Charity.

This section applies to all employees, contractors and volunteers at RCL who use the internet in work time to access key RM applications and programmes. It applies no matter whether that internet access takes place on RCL premises, while travelling for business or while working from home.

It applies to use of the internet on any device that is owned by RCL, or that is connected to any RCL networks, systems or applications. For example, it applies both to an employee using the internet at their desk, and to employees who connect their own tablets or smart phones to RM applications.

- Users must not participate in any online activities that are likely to bring the Charity into disrepute. Create or transmit material that might be defamatory, or incur liability on the part of the Charity, or adversely impact on the image of the Charity.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the Charity's computer network.
- Users must not "hack into" unauthorised areas.
- Users must not download, publish or share commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement, or other such licence.
- Users must not use the internet for personal financial gain.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism or fraud.

- Users must not use the internet to send offensive or harassing material to other users.
- Use of gambling sites, online auction sites is not permissible.
- Users must not use RCL's equipment, software or internet connection to perform any tasks which may involve breach of copyright law.
- Staff may face disciplinary action or other sanctions (see below) if they breach this policy and/ or bring embarrassment on the Charity, or bring it into disrepute.

Reasonable personal use is permissible also subject to the above and must not cause an increase for significant resource demand, e.g. storage, capacity, speed, or degrade system performance. It must be limited, reasonable, and done only during non-working hours (e.g. lunch-time).

SOCIAL MEDIA

RCL employees / volunteers / contractors may be able to access social media services and social networking websites at work, either through RCL systems or via their own personal equipment.

RCL has a separate detailed Social Media policy which includes guidance, best practice, safeguarding controls and responsibilities for all employees, volunteers and contractors.

The policy (along with our data protection policy) can be obtained by emailing admin@revelationchurch.org.uk.

LEGITIMATE ACCESS TO PROHIBITED MATERIAL

If an employee feels that the nature of their work requires them to access or use material prohibited under this policy, they should discuss this with their Line Manager. The Charity is legally responsible for the content and nature of all materials stored on/ accessed from its network.

HEALTH AND SAFETY

RCL has a duty of care to its employees, volunteers and contractors to ensure they are kept safe whilst engaging in activity on behalf of RCL.

In terms of ICT, this usually relates to visual display units (VDUs), electrical equipment testing, office and home working. Rules and regulations are outlined on this by the Health & Safety Executive - www.hse.gov.uk/office/

RCL has a risk assessment process in place to assess each of these areas, though individuals are encouraged to discuss any requirements they have in this regard with the owner of this policy.

POLICY ENFORCEMENT AND MONITORING

All resources of the Charity (where RCL 'owns' or has provided / contributed financial resources to ICT resources), including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the Charity then, at any time and without prior notice, the Charity maintains the right to examine any systems and inspect and review all data recorded in those systems.

This will be undertaken by authorised staff only.

Any information stored on a computer, whether contained on a hard drive, USB device, or in any other manner, may be subject to scrutiny by the Charity. All data written, sent or received through RCL's 'owned systems' is part of official RCL records. RCL can be legally compelled to show that information to law enforcement agencies or other parties if requested.

This examination helps ensure compliance with internal policies, and the law. It supports the performance of internal investigations, and assists in the management of information systems.

All individuals authorised to use RCL's infrastructure should always ensure that the business information sent over or uploaded is accurate, appropriate, ethical, and legal.

DISCIPLINARY ACTION AND PENALTIES FOR IMPROPER USE

Knowingly breaching this policy is a serious matter.

Employers / Volunteers / Contractors who do so will be subject to appropriate disciplinary action according to agreed contracts. They may also be held personally liable for violating this policy, according to the nature of the breach. Disciplinary action may consist of:

1. ***Withdrawal of facilities:*** Users in breach of these regulations may have access to Charity IT facilities restricted or withdrawn.

2. ***Disciplinary Action:*** Breaches of these regulations may be dealt with under the Charity's disciplinary procedures, and could lead to termination of employment from the Charity.

3. ***Breaches of the law:*** Breaches of the law will be reported to the police, where appropriate