



IT, Email and Social Media Policy

Excel Church recognises that the internet, email, and related technologies are essential business tools, providing vital means of communication and access to information and resources.

Proper and appropriate use of these resources is essential to ensure the Church's integrity, security, and productivity. The purpose of this policy is to clearly set out the expectations regarding the acceptable use of IT systems and to minimise the risk of inappropriate or unlawful behaviour when utilising these resources.

All users must familiarise themselves with and comply with this policy. The policy should be read in conjunction with Excel Data Protection Policy. [Data Protection Policy](#). Failure to comply may lead to disciplinary action.

If you are unsure whether a particular action may breach this policy, please consult your line manager or the data controller Daniel Lee before proceeding who can be contacted via this link [Dan Lee](#).

Any breach of this policy will be treated as misconduct and may lead to temporary or permanent revocation of IT access or in serious cases disciplinary action.

All IT equipment issued by the Church, including mobile phones, remains the property of the Church.

Security of IT Equipment and Data

Employees, contractors and volunteers are responsible for the security of any IT equipment assigned to or used by them and must take reasonable steps to prevent theft, loss, or damage. Intentional damage, interference, or unauthorised access to the Church's IT systems may result in disciplinary action,

Any loss, theft, or damage of IT equipment or data storage devices must be reported immediately to the data controller.

Laptops must be stored securely when taken off-site and should not be left unattended. In exceptional circumstances if a laptop has to be left in a vehicle it should always be in a locked boot. All devices must be protected by secure passwords or biometric authentication.

Employees, contractors and volunteers are responsible for safeguarding Church data, including personal and sensitive data related to clients, suppliers, and colleagues. You must familiarise yourself with your obligations in the Data Protection



Policy. Portable devices, such as USB drives and smartphones, must be securely stored and always encrypted.

Virus Protection

To prevent virus and malware threats:

- Only authorised software may be installed.
- External media (USBs, CDs, downloads) must be used in line with current procedures.
- When appropriate software must be virus-checked before installation.

When appropriate antivirus software is installed and updated regularly. However, users are expected to act responsibly and avoid activities that could introduce viruses to Church systems.

Any breach of these procedures may result in disciplinary action.

Software Policy

Only legally acquired and licensed software may be used. The installation of software must only be carried out by authorised personnel.

Employees and volunteers must not:

- Copy, distribute, or install software without a valid licence.
- Make or share unauthorised copies of Church software.

Breaches may result in disciplinary action, including dismissal.

Harassment and Bullying

Church IT systems must not be used to engage in, support, or promote harassment, discrimination, or bullying of any kind.

Email and internet use must align with the Church's commitment to equality and respect, including protection from harassment based on race, gender, sexual orientation, age, disability, religion, or other protected characteristics. Offensive or discriminatory material must not be created, accessed, stored, or distributed. Violations may lead to summary dismissal.

Deleted emails may be recoverable and may be used as evidence in legal or disciplinary proceedings.

Email Usage



Church email accounts are provided for business use. Personal use of church email accounts may be authorised by the data controller [Dan Lee](#).

Email usage must adhere to the following principles:

- All communications should reflect professionalism and courtesy.
- Emails should be reviewed for accuracy before sending.
- Confidential or sensitive information must not be shared externally without authorisation.
- Emails should not be used to transmit:
 - Defamatory, offensive, or inappropriate content
 - Pornographic or obscene material
 - Confidential or embargoed information
 - Copyrighted material without permission
- Chain letters, "junk mail," and mass personal emails must not be sent.
- Email attachments from unknown sources must not be opened.
- Messages must be directed only to those who need the information.

All messages, including deleted items, may be monitored or retrieved. Misuse may result in disciplinary action.

Internet Usage

Limited personal use of the internet by employees, contractors and volunteers is permitted during non-working hours (e.g. lunch breaks), provided it does not interfere with work responsibilities or breach Church policy.

Additional rules:

- Accessing or distributing inappropriate content (e.g. pornography, gambling, hate speech) is strictly prohibited.
- Confidential Church information must not be transmitted over unsecured platforms.
- Copyrighted material must not be downloaded or shared unlawfully.
- Internet usage may be monitored, and excessive or inappropriate use may lead to disciplinary action.

Social Media and Blogs

Social media is a valuable tool for outreach and communication. However, employees, contractors and volunteers must use it responsibly and **must not**.

- Post defamatory, discriminatory, or abusive content.
- Share confidential or proprietary information.
- Post content that could damage the Church's reputation.



A clear boundary must be maintained between personal and professional life on public platforms.

Permission must be sought prior to posting pictures of children or adults at risk in accordance with [Photo and Video Policy](#).

If in doubt about content, consult you're the data controller before posting.
Violations may result in disciplinary action.

Account Access and Password Management

Individuals who have access to official Excel Church social media accounts must not change account passwords or linked email addresses without prior authorization from the Data Controller [Dan Lee](#)

- All current passwords and login details must be recorded and securely stored in the church's official Social Media Register.

Creation of New Accounts

No new social media accounts representing Excel Church or any of its ministries, departments, or groups may be created without prior written approval from the Excel Church Trustees.

- This ensures all accounts are consistent with the church's mission, branding, and safeguarding standards.

Official Church Email Requirement

All Excel Church social media accounts must be registered using an official Excel Church email address, ideally one dedicated to communications or IT management (communications@excelchurch.org.uk).

- Personal email addresses must not be used to create or manage church social media accounts.
- This helps maintain accountability, continuity, and security in case of staff or volunteer transitions.

Administrative Oversight

The Data Controller will keep a register of who has access to social media accounts and will periodically review account access and permissions to ensure they remain appropriate and up to date.

Ownership and Continuity



All social media accounts created on behalf of Excel Church remain the property of Excel Church, not of the individual who created or manages them.

Transition Procedure

When a staff member or volunteer with access steps down, passwords must be updated and recorded in the Social Media Register, and access removed promptly.

A register will be kept of who has access to church social media accounts and what their level of access is. Access will be given where the role requires it and will be reviewed regularly.

Telephone Use

Church phones are for business use. Personal calls should be limited to essential matters and kept brief (no more than 5 minutes, except in emergencies). Excessive personal use may result in reimbursement of call charges and disciplinary action. Text messages must follow the same standards as email communication. The Church may reclaim supplied mobile phones at any time without notice.

Voicemail

Voicemail should not be used as a substitute for answering calls. When using voicemail:

- Ensure your greeting is professional and up to date.
- Consider deactivating voicemail if a colleague is available to take messages.

Use of Cameras and Video on Devices

The use of camera or video functions on smartphones must comply with [Excel Photo and Video Policy](#). Capturing or sharing inappropriate content is strictly prohibited. Any misuse may result in disciplinary action.

Monitoring and Privacy

The Church may monitor all IT activity, including:

- Emails (incoming/outgoing, internal/external), even if marked “personal”.
- Internet usage and website visits
- Mobile device and system access logs



Monitoring is carried out in accordance with the Data Protection Act 2018 and UK GDPR. By using Church systems, you consent to this monitoring. Church emails and files remain the property of the Church. Users should not expect privacy when using Church systems.

Compliance

Employees, contractors and volunteers must comply with this policy at all times. The Church reserves the right to revise this policy periodically. Staff and volunteers will be informed of any updates and must ensure they are aware of the current version. Breaches of this policy may result in disciplinary action, up to and including dismissal or removal from volunteering.

Document Acknowledgement

By signing this document, you acknowledge that you have read, understood, and agree to comply with the Church's IT and communications policy.

Signed

Date