IT, Email and Social Media Policy

The Church recognises that the internet and email are important business tools, providing communications and access to information, resources and ideas.

Proper and appropriate use of these resources is of the utmost importance to the Church. The purpose of this policy is to clearly communicate expectations in respect as to what constitutes 'proper and appropriate' use, and to minimise the risk of offensive or inappropriate behaviour when utilising these resources.

These policies are designed to prevent problems with IT use and therefore, you are required to be familiar and comply with the contents of this policy.

If you are unsure about whether anything you propose to do might breach this policy, you should speak to your manager.

Any breach of this policy will be viewed as misconduct and may result in disciplinary action being taken against you. This could include your access to the Church's email facilities and the internet being suspended or withdrawn, or, in serious cases, dismissal without notice or pay in lieu of notice.

Any IT equipment allocated by the Church to the employee remains the property of the Church, including mobile telephones.

Security of IT Equipment and Data

Employees must endeavour to safeguard any IT equipment assigned to them and make every effort to prevent theft and damage.

Vandalism of, or otherwise intentionally interfering with, the Church's computer network constitutes a gross misconduct offence and may result in disciplinary action.

Loss, theft or damage of IT equipment or data storage devices must be reported immediately to the Church.

Laptops must be kept in a secure place when taking away from the Church's premises. They should not, for example, be left in vehicles overnight or in other places where they are likely to be at risk of theft or damage. All laptops must be password protected.

Employees have a responsibility for ensuring the safeguard of Church data, which includes data relating to clients, suppliers and employees. Portable devices such as memory sticks or mobile telephones/smartphones should be kept in a secure place at all times, as they are likely to hold Church data, they should also be password protected. The loss of data and IT equipment is a potentially serious matter and employees must always ensure that safeguarding this is a priority.

Virus Protection
In order to prevent the introduction of virus contamination into the software system, the following must be observed:

- Unauthorised software including public domain software, discs, CDs or internet downloads must not be used without prior permission from the person responsible for IT.
- All software must be virus checked by the person responsible for IT using standard testing procedures, before being used.

Although antivirus software is installed on relevant church computers and updated from time to time, it is the personal responsibility of all computer users to ensure that they do not introduce viruses into computer systems, and that they carry out regular virus checks on their own system.

Breach of these virus protection procedures may result in disciplinary action that may lead to dismissal.

Software Policy
The Church is committed to the use of authorised software only within its computer systems. It is our policy not to use any pirated or illegal software. Any software used on Church premises or on Church hardware must have been legally acquired, and the use of such software must comply with all aspects of the related software purchase agreement. Software installation must only take place by authorised individuals.

You must not make 'pirate' copies of Church owned software for use by other persons either inside or outside the Church. This not only breaks Church rules but it is an illegal practice.

Acting in breach of this requirement could result in disciplinary action up to and including dismissal.

Harassment and Bullying
Church email and the internet shall not be used to violate the Church's commitment to respecting the dignity of all employees and providing a professional environment in which they can develop their careers.

This will be without fear of harassment, bullying or victimisation due to race, colour, religion, belief, sex or sexual orientation, marital status, pregnancy, age, national origin, disability, medical condition, or any other consideration made unlawful by UK laws.

Employees who harass or bully fellow workers may be dismissed on the grounds of gross misconduct.

Deleted emails may still be recoverable and are regarded as legitimate forms of evidence in court.

Email

The Church provides email facilities to individuals for the purpose of conducting Church business.

Incidental personal use is permitted subject to use being limited at lunchtime and other breaks and never taking priority over work matters or interfering with the individual's work responsibilities. Where employees regularly spend excessive time 'chatting' by email for personal and private purposes, this will be brought to the employee's attention via the Church's disciplinary procedures. Employees are also prohibited from using email to circulate any non-work material.

Messages sent over the email system can give rise to legal action against the Church. Claims of defamation, breach of confidentiality or contract could arise from a misuse of the system. In addition, the use of email attachments whilst adding value can harm a Church (e.g. viruses). It is therefore vital for email messages to be treated like any other form of correspondence and where necessary hard copies to be retained. Email messages are disclosable in any legal action commenced against the Church relevant to the issues set out in the email.

When sending internal or external emails, employees should comply with the following:

- All client and customer communications (incoming and outgoing) should be recorded on file (hard copy or electronic files dependent on protocol) in the same way as a letter or fax.
- Emails which have been incorrectly delivered to an employee's email address should be redirected to the intended recipient and the sender. If the email contains confidential information this must not be disclosed or used. If you receive an email which contravenes this policy the email should be brought to the attention of your line manager.
- Emails should be checked thoroughly before sending (including checking that they have been properly addressed) to the same standard as hard copy communications and letters.
- Messages sent on email systems are to be written in accordance with the standards of any other form of written communication and the content and language used in the messages must be consistent with best practice.
- Emails sent internally may be sent in an informal style, but employees are asked to observe the normal courtesy that they would extend in written memos as the house style. An example of an acceptable style is available if required.
- Messages should be concise and directed to those individuals with a need to know. General messages to a wide group should only be used where necessary.
- Any emails containing references to or evidence of Church activities and arrangements should be preserved and saved for reference.

Employees must not:

- Use internal or external emails for any material, which could potentially be defamatory. Examples of this include statements which are untrue, malicious or otherwise, or inappropriate comments about customers, competitors or other employees.
- Initiate or forward emails that contain obscene or pornographic material.
- Disclose information that is protected by embargo or could in any way be considered confidential to the Church and/or employees. Confidential information should not be sent externally by email without express authority from the Lead Pastor.
- Make any statements via email which intentionally or unintentionally creates a binding contract or make negligent statements.
- Send general personal messages to a large number of addressees.
- Use emails for the distribution of obscene and/or offensive material in any form.
- Respond to "junk mail".
- Send 'fun' emails, as what may seem harmless fun to some can be offensive to others and may be regarded as harassment. If employees receive an email which they consider offensive, they should raise the issue with line management.
- Respond to, or forward on, chain letter type emails.
- Download any games onto the system or play any games they receive.
- Import unknown messages, files or attachments onto the system without authorisation.
- Send attachments by email without obtaining the consent of the author of the attachment if not an employee as this may entail an infringement of copyright. Bear in mind that, in some cases, recipients can view previous changes to attachments.
- Employees must not open any emails from unknown sources as this is how most viruses are introduced and can easily spread throughout systems.
- Send large graphic or video files unless they are related to the Church's activities.

Internet

Limited personal use of the Internet should be restricted to out of office hours such as lunch breaks, unless the permission of your line manager has been sought and given for that one off purpose.

All relevant points covered in the email section above are to be applied to the internet.

Additional points are:

- Breach of this internet section will be viewed as misconduct and may result in disciplinary action being taken against you including, in serious cases, dismissal without notice or pay in lieu of notice.
- Use of the internet for inappropriate purposes (e.g. downloading pornography or using the internet for gambling or illegal activities) will be regarded as gross misconduct, justifying instant (summary) dismissal.
- Confidential information should never be sent via the internet.
- Work protected by copyright must not be downloaded, copied or sent via the internet or email.

- We may choose to monitor internet usage and specific sites accessed where we suspect the above guidelines are being breached.

The law with regard to email and internet access and use is still evolving. This policy takes into account the current legal situation but employees should be aware that it will continue to change, often at great pace. For this reason, staff will be notified of any changes and they must ensure they update themselves regularly with the current version of this policy that is available on the Church intranet.

Social Media Sites and Blogs

Social media is an increasingly important communication tool for Churches. It is a particularly useful medium within professional services for building relationships and creating brand awareness. This policy is aimed at setting out how Excel Church employees can use social media to support church activities.

We have the opportunity to build awareness of our church through social media channels. It should be noted that members of the congregation attend our church because they believe in what we do. Our social media activity should support the ethos of building trust with our congregation and the wider community.

In addition, whilst we respect your right to a private life, we must also ensure that our confidentiality and our reputation are protected. If you are using social media websites out of work times you must use common sense at all times, and in particular, you must:

- Ensure you never send abusive, defamatory or discriminatory messages or associate yourself with anything that may be considered abusive, defamatory or discriminatory.
- Ensure that you do not conduct yourself or communicate information in a way that is detrimental to the Church or may damage working relationships between members of staff, relatives, members of the congregation, suppliers or others who have relationships with the Church. This includes, for example posting identifiable comments about feelings towards work or work colleagues and/ or issues at work;
- Ensure that no information is made available that could provide a person with unauthorised access to the Church or other Church employees, relatives, supporters or suppliers This includes, for example, making Church related contacts identifiable as public list of friends in Facebook or contacts in LinkedIn;
- You may not share information that is confidential and proprietary about the Church. This includes information about trademarks, upcoming proposition developments, sales, finances, clients, Church strategy and any other information that has not been publicly released by the Church.
- These are given as examples only and do not cover the range of what the Church considers confidential and proprietary. If you have any question about whether information has been released publicly or doubts of any kind, speak with your manager before releasing information that could potentially harm our Church, or our current and potential services, employees, partners and clients. You may also want to be aware

of the points made in the non-disclosure agreement you signed when you joined our Church.
- Report any concerns about any matters relating to your use of social media sites which may affect the Church to your manager at the earliest opportunity.

Any breach of these guidelines may lead to disciplinary action being taken against you, up to and including the termination of employment.

You should be aware that many websites are a public forum, particularly if you are part of a 'network'. You should not assume that your entries on any website will remain private.

Telephone

The Church's telephones are for the exclusive use by employees in connection with the Church's business. Employees may be issued with a mobile phone at the discretion of their manager where the employee requires a mobile phone for business use.

Additional accessories and car kits may be available.

Whilst the Church will allow essential personal telephone calls concerning an employee's domestic arrangements, excessive use of the telephone for personal calls is prohibited. We expect essential domestic calls to be limited to 5 minutes duration apart from in emergency situations. Where such use is discovered, employees will be required to pay to the Church the cost of the personal calls made.

When sending text messages, employees are bound by the same guidelines regarding content of messages as for the policy on sending emails (above).

The Church may demand the return of the phone on either a temporary or permanent basis at any time and without notice. The employee is not entitled to any compensation should a mobile phone be withdrawn.

Voicemail Policy

Voicemail must never be used in preference to answering an incoming call.

With any communication tool it is essential that it be used in a consistent manner across the Church in order to be effective. With this in mind we have set out the following guidelines when using the system:

- Use of voicemail during normal office hours is not compulsory. If you intend to be away from your desk for short periods of time during the day you may choose to activate your voicemail to intercept incoming calls, or alternatively leave voicemail deactivated to allow messages to be intercepted by a colleague.
- When using voicemail either during the day or outside normal office hours, please ensure you record a suitable greeting message.

Camera / Video Camera Phone Policy

The above applicable guidelines relating to appropriate email and internet usage must be observed in relation to the use of such camera/ video camera equipment or functions of smartphones. Any employee found in violation of the policy may be subject to disciplinary action up to and including the termination of employment.

Monitoring and Privacy

The Church has the authority and ability to intercept, open, read and print out all internal and external (incoming and outgoing) emails, including those marked 'personal'. The Church complies with the Data Protection Act 1998. The Church is obliged to inform you that your emails may be intercepted without your knowledge and by signing this document you acknowledge that you have given your consent to this.

The Church also has the authority and ability to access, read and print out details of all internet sites accessed by persons using its computer systems. The Church reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it.

The Church considers that valid reasons for checking an employee's internet usage include suspicions that the employee has breached any of the above rules regarding internet usage. The Church reserves the right to retain information that it has gathered on employees' use of the internet for an appropriate amount of time and in accordance with Data Protection legislation.

Email messages are the property of the Church. Employees should have no expectations of privacy with respect to the use of the internet or email from search sites and/or devices.

You agree that the Church may take all actions necessary to ensure that this policy is adhered to.