KING'S LYNN CHRISTIAN FELLOWSHIP

ALSO KNOWN AS THE KING'S CENTRE

IT POLICY

Responsibility

The Office Manager has overall responsibility for all matters related to IT.

The Office Manager may delegate responsibilities or tasks to other employees or volunteers but will retain overall responsibility for ensuring that the requirements of this policy are carried out.

Users

A user is defined as anyone who uses any church-owned devices or facilities, whether an employee or a volunteer, in order to undertake tasks related to the running of the church.

All users will be required to sign to say that they have read and understood The King's Centre Acceptable Use Policy for equipment, systems and facilities.

Anyone who is granted access to the church management software solely for managing their own details, and those of their family, will not be regarded as a user.

For the purposes of this policy, anyone who simply uses guest access to the church wi-fi network during services or meetings is not regarded as a user.

When the building is hired out, hirers must comply with the section in the Hire Policy that relates to the use of mobile phones, cameras and other electronic devices.

Church-owned devices

This includes, but is not limited to, desktop computers, laptops, tablets, phones, projectors and printers.

There is an inventory of church-owned devices showing dates of purchase and expected replacement dates to inform a planned replacement programme.

The Office Manager keeps a list of all administrator and user logins and passwords for each device.

Each device should have a nominated person responsible for routine housekeeping.

All devices should be kept up to date with the latest software updates.

Firewalls should be active on all devices.

All devices must be accessible only by use of a login and password. Where devices are shared by more than one person, each person should have their own login and password.

Church-owned devices may be taken off the King's Centre premises only with the express permission of the Office Manager. If devices are required for use elsewhere (such as an alternative location for church services or other events), the Office Manager must approve these storage locations in advance.

Equipment must be insured if taken off premises, either through the church insurers or by the person borrowing the equipment.

Users may not install any software onto church equipment without the express permission of the Office Manager.

Provision of IT resources for employees

The trustees recognise that employees should be given the IT resources to enable them to do their jobs. Where this requires the use of a desktop, laptop, tablet or mobile phone, the church will provide the

necessary hardware, software and backup facilities. Devices may be shared by two or more employees, where appropriate.

Trustees recognise that employees may prefer to purchase their own personal IT equipment and use this for church work, rather than having a separate computer or other device provided by the church purely for church work. This may be because the employee wishes to have a device of a higher specification, for example.

In approved cases, trustees will make a payment to the employee for the cost of a new electronic device that would be adequate for their work requirements. The device would be the property of the employee, who would be responsible for insuring it. When the device needs to be replaced, which would not normally be sooner than 5 years from the date of purchase, a further payment will be made if the employee wishes to own a replacement device. The employee must sign an undertaking that if they leave within the 5-year period that they will reimburse the church 20% of the original sum given for each year that remains of the 5-year period.

Where employees use their own devices, the church will pay for all necessary software and backup facilities.

Employees may use equipment provided by the church for personal use if they wish, in accordance with the Acceptable Use Policy.

Provision of IT resources for volunteers

The trustees recognise that volunteers may require IT resources to enable them to fulfil their roles. Decisions about provision of equipment or payments towards the costs of volunteers' own devices will be made on a case-by-case basis.

Devices not owned by the church but used for church purposes

Employees or volunteers may bring their own devices onto church property in order to fulfil their roles, but they must ensure that they follow the Acceptable Use Policy.

Employees or volunteers who use their own devices away from church property in order to fulfil their roles must ensure that they follow the Acceptable Use Policy.

The church IT infrastructure, including routers, switches and wi-fi networks

Church IT infrastructure, including routers, switches and wi-fi networks, should be configured and maintained in such a way as to ensure security for devices and data.

Software and software licences

All software used for church purposes, whether in the church building, using church-owned devices or on employees or volunteers' personal devices, should be kept up to date and with appropriate licences in place.

Arrangements for backing up data

All data files in connection with church purposes, whether on church-owned devices or on employees or volunteers' personal devices, should be kept secure and backed up in a separate location (preferably in the Cloud or on storage media kept in a separate building). Ideally this should be on the Cloud and managed by, and accessible to, the Office Manager. However, confidential data may be backed up separately.

Where employees or volunteers make their own arrangements for backing up data, the Office Manger must be informed about how this data can be accessed in a crisis.

In the event that an employee or volunteer ceases to perform a particular role, all relevant files should be made available to the Office Manager for the use of those taking on that role.

Digital safety and cyber security

Employees and volunteers should take all necessary steps to ensure that church data is kept securely, and to prevent unauthorised people from accessing that data.

Employees and volunteers will be required where appropriate to undertake relevant training arranged by the Office Manager.

Employees and volunteers should alert the Office Manager immediately if they suspect that there has been a data breach or that security may have been compromised.

Church website and social media accounts

The Office Manager is responsible for the regular updating and maintenance of the church website, to ensure that information is up-to-date and relevant.

The Office Manager is responsible for ensuring that church social media accounts are managed appropriately.

Church management software and communications

The Office Manager is responsible for all aspects of the church management software, including regular updating and maintenance, managing users, disseminating information and providing support for users.

The Office Manager is responsible for overseeing the sending of emails to those on the email database and for maintaining that database in accordance with the General Data Protection Regulations (GDPR).

The Office Manager is responsible for the day-to-day operation of the GDPR.