INFORMATION SECURITY POLICY

POLICY STATEMENT

This is the Information Security Policy of King's Community Church which serves the community with various activities and also hires out conference facilities and has a coffee shop. King's Community Church is often just known as "King's" and it is that name that will be used throughout the rest of this document.

Background

This policy details the information security measures we have in place to protect the confidentiality, integrity and availability of our information assets, the data we process, and to facilitate the rights of the individuals to whom personal data relates.

We do this through implementing systems and procedures to minimise the risks of malware attacks, unauthorised access to our systems and potential compromise of the data contained within them.

PHYSICAL & VIRTUAL ACCESS

Physical Access

Staff are issued keys to the premises, depending on their role and responsibilities. Details of keyholders are recorded. Keys are to be returned upon termination of employment or end of contract.

Physical documentation containing personal data is stored in locked filing cabinets; this also includes data that is usually stored electronically but has been printed out. Personnel who are authorised to access the personal data stored in our physical filing systems are detailed on the User Access Log, which is separate to this policy document.

Virtual Access

Only authorised staff/ volunteers will be permitted access to King's computer systems. Their access will be revoked upon termination of their contract/ services.

See section on User Access Control for further information.

Clear Desk & Clear Screen Policy

Clear Desk

If leaving desks unattended, all paperwork containing personal or sensitive data is to be cleared away to prevent access by visitors or unauthorised individuals.

Sticky notes containing passwords or personal data must not be attached to/ visible on desks and/ or screens.

Clear Screen

If screens are left on but unattended, they must be locked to prevent access by unauthorised individuals; they can then be unlocked when the user returns to the screen. If users need to leave their screens for more than a few minutes, or at the end of their working day, they must log out.

If printing documents containing personal or sensitive data, they must be taken from the printer immediately and not left and collected at a later time.

User Access Control

Access to King's computers and systems is on a 'need to access' basis with all users recorded on the User Access Log.

New staff/ volunteers will be granted access to the systems necessary to perform their job, with an access level appropriate to their role and responsibilities.

Strong passwords should be used and contain a combination of upper and lowercase letters, numbers and symbols; passwords should not be shared or written down.

When an employee/ volunteer leaves at the end of their contract, their user access is revoked.

Secure Configuration

Secure configuration refers to security measures that are implemented when building and installing computers and network devices, in order to reduce unnecessary security vulnerabilities.

King's policy is to protect the confidentiality, integrity and availability of the data we process and contain within our systems. We do this by paying for a third party (NetMatters) to manage our computer network.

Firewalls

A firewall is a software application, or combination of software and a hardware device, in place to examine, filter and control network traffic flow to and from the computers and network, and to allow authorised communications and prevent unauthorised or malicious access or communications.

NetMatters has installed firewall protection on our network and on all our computers that process and store personal data.

Encryption

King's minimises the personal data we send electronically and only does so when absolutely necessary.

Malware Protection

Malware is malicious software that is designed to infect computers and devices and inflict harm upon their processes and corrupt or steal the data stored within them. Malware has become increasingly sophisticated, therefore robust malware protection on all devices is essential.

NetMatters has installed malware protection software on all computers.

Security Patch / Update Management

A security patch is a piece of software designed to update, fix or improve an existing application on your computer or device. Some patches improve the security and/ or efficient working of the program to which it relates, so it is essential to install any patches/ updates when notified.

NetMatters ensures that all our devices are kept up-to-date with the latest updates and patches;

Backups and Disaster RecoverY

Backups and disaster recovery are essential under the GDPR, to ensure the availability and access to personal data in a timely manner in the event of a physical or technical incident.

NetMatters manages all King's backup and recovery procedures.

Backups are performed of our servers: KC-RDS-01 - Every day at 22:00 , KC-DC-01 Every day at 20:00 and these retained for [1] months before being overwritten.

Upon completion of backups, media copies are stored in secure locations. All media is logged and dated to enable quick recovery in the event of an incident.

Incident Management / Data Breach

Situations that constitute a security incident include, but are not limited to, the following:

- an adverse event that causes accidental or malicious loss or destruction of data contained within the IT system in question, or alteration or access of the data in respect of availability, integrity and confidentiality of the data;
- unauthorised access to systems used by King's resulting in disclosure of confidential information;
- a malware attack or attempted unauthorised access to any of our internal or external IT systems;
- staff disclosure to unauthorised persons of confidential data.

While all data breaches are considered an information security incident, not all information security incidents constitute a data breach; under the GDPR a data breach in only when *personal* data is affected.

If you believe there has been a data breach, please notify the King's Data Representative (data@kings-norwich.com) immediately who will assess the breach and invoke the Data Breach Notification Procedure if necessary.

Staff Training

All new staff and volunteers will undergo Information Security guidance and awareness training; existing staff will undergo refresher Information Security training on an annual basis. All training will be recorded on the training record to facilitate easier management of training requirements.

Last Updated 9/2/23 by the GDPR Team