|  |  |
| --- | --- |
|  | Morningside United Church15 Chamberlain RoadEdinburghEH10 4DJScottish Charity Number - SC015552 |

Information Security Policy

## Confidentiality, integrity, availability and resilience are the foundational elements of information security.

**GDPR now makes it an obligation for all organisations to undertake tests of security measures on a regular basis.** Importantly, it does not specify the type of testing, nor how regularly we should undertake it. It depends on our church circumstances and the personal data we are processing.

Whatever form of testing we undertake, we should document the results and make sure that we act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if our testing reveals potential critical flaws that could result in a personal data breach.

## Management and organisational information security

The Kirk Session is responsible for:

* Identifying and managing information security risks (1.1)
* Creating an Information security Policy which is regularly reviewed and complies with all relevant laws (1.2)
* Identifying a person to take responsibility for information security (1.3) – The data Protection Officer

## Our staff and information security awareness

We will regularly train staff to ensure that they are aware of security issues. (2.1)

## Physical security

We have established entry controls to the main entrance to the halls, the church office, the vestry and the basement (3.1). Entry from the church flat to the halls is also controlled. These coded controls are disclosed only to those who need to know them. These measures prevent unauthorised access to areas that need to be protected.

We have secure storage areas to protect equipment and data (3.2)

We have established a process to securely dispose of records and equipment when no longer required (3.3).We shred of paper records when no longer required. Equipment no longer needed is disposed of securely.

We endeavour to ensure that the church office and vestry, when open, are not left unattended. A door closer has been attached to the office door.

## Computer and network security

1. To have a hardware and software asset register with assigned responsibilities is unnecessary given our limited assets. (4.1)
2. Staff and office bearers are not issued with mobile devices specifically for church business (4.2)
3. We will configure computer hardware so as to reduce vulnerabilities such as unnecessary accounts or default passwords and to provide only the software necessary (4.3)
4. We will control the use of removable media by ensuring that personal data on such media is kept securely on media which is church property and used only for the purpose intended. No personal devices should be attached to church IT property. (4.4)
5. Special user accounts are unnecessary (4.5)
6. Passwords will be changed regularly (4.6)
7. We have installed anti-virus software on all devices (4.7)
8. We have a backup and recovery procedure and business continuity plan (4.8)
9. Routine logging of user activity unnecessary (4.9)
10. Security patches are regularly applied to all devices (4.10)
11. Firewalls are in place (4.11)
12. Files containing personal data will be encrypted and password protected
13. When password protecting a new file, that password must be shared with at least one other appropriate person
14. Removable media such as memory sticks must not be inserted into church equipment unless such media is the property of the church

**Testing and business continuity plan**

Each week, backup all folders on the office computer to a memory stick.

As a test for business continuity purposes, once a year, delete all data folders on the church office computer and restore them from backup to both the church computer and another computer.

Consider what would happen if software programs were corrupted or deleted. Could they be reinstalled?