1 Introduction

1.1 Foundation Scotland [FS] recognises that information is one of the most important assets it needs to manage. Specifically, FS must:

- Maintain confidentiality: protecting information resources from unauthorised individuals and organisations
- Ensure availability: allowing employees to carry out their work unhindered
- Maintain information integrity: ensuring the data is complete and correct

1.2 Cyber Essentials Accreditation is one important way that FS ensures that it is working to the highest possible data security standards. Other ways that FS protects its information assets are detailed in the policy below.

2 Scope

2.1 This policy applies to all systems, people and processes that constitute FS's information systems, including board members, committee members, employees, suppliers and other third parties who have access to FS's systems.

3 Abbreviations and Definitions

Abbreviations

- CFOO – Chief Finance and Operations Officer
- GDPR – The General Data Protection Legislation
- ICO – Information Commissioner's Office
- LMS – the FS Learning Management System
- Microsys – FS's IT and telephony partner

4 Policy

Acceptable Use Policy

4.1 FS is committed to protecting its employees and the information assets of the organisation from illegal or damaging actions by individuals, either knowingly or unknowingly. FS supplied equipment is to be used for work purposes only during the working day. Personal use is allowable out of work hours and employees are expected to use good judgement in its usage. Issues of an employee found to be using FS equipment for unlawful purposes or for purposes which would bring FS into disrepute, will be managed through the Disciplinary policy.

Anti-virus Software

4.2 Trend-Micro is used by Microsys to protect all FS laptops and the Finance Server. Security updates are deployed when needed and employees are unable to switch off updates.

Automatic forwarding of Email

4.3 Email must never be automatically forwarded to a non-FS email address. Non-automatic forwarding of email to addresses outside of the organisation must be done with care to ensure that any sensitive information is removed.

Bluetooth Requirements

4.4 FS laptops do not have Bluetooth functionality enabled. Permission to enable it must be approved by FS [in practice the CFOO].

"Clear Desk" at Home

4.5 All FS employees are required to ensure that all confidential/sensitive information in either paper or electronic form is secure at their work area or if they are expecting to be away from their work areas for an extended period. Laptops should be locked when away from the work area and must be shut down completely at the end of the day. If possible, laptops should be stored securely, out of sight, when not in use.

Confidentiality Agreements [also known as NDA's – Non-Disclosure Agreements]

4.6 FS has a standard NDA for use when it is working with an external party and wishes to share confidential information to enable the party to undertake the work. NDA's are drafted by the CFOO.

Cyber Essentials

4.7 As part of its desire to operate in the most digitally secure manner possible, FS has taken the decision to be Cyber Essentials Accredited. The annual review process is undertaken by Microsys on our behalf.

Data Backup and Business Continuity Planning [BCP]

4.8 The BCP details the frequency and process by which FS systems should be backed up locally. The Finance server is held at Microsys's office and back-up protocols have been agreed with them.

Data Breaches

4.9 All data breaches should be notified to the CFOO without delay, logged on RiskMate, and action taken immediately to minimise any hurt to data subjects. In accordance with GDPR law, serious breaches must be notified to the ICO. Should this be required the CFOO will liaise with the CEO as per the Data Protection Policy.

Digital and Electronic Signatures

4.10 Both digital and electronic signatures are acceptable within FS. FS may sign documents digitally which are sent from suppliers and clients.

Email Policy and Retention

4.11 An FS email address must be used for work purposes only. It is acceptable however to use FS equipment to access personal email accounts during the working day during breaks. Employees must ensure that emails containing information which relates to a Data Subject are removed and stored on the CRM to ensure that they can be managed in accordance with agreed retention periods and are accessible to other employees, if needed.

Equipment Registers and Security

4.12 All equipment supplied to employees for working at home will be logged on their Breathe records. It is the responsibility of FS employees to ensure that they take care of all equipment issued and report any damage or loss immediately to the CFOO.

Firewall

4.13 Firewall is enabled on Office gateway router. Firewall is enabled for devices through Trend Micro Agent and Windows Firewall is enabled.

Mobile Phones

4.14 Work mobile phones are supplied to staff who travel frequently. These are all password protected and have "find my device" enabled. Staff may use personal devices to access emails however it is a requirement that these be password protected.

Password Protection

4.15 Passwords must be strong, Cyber Aware - NCSC.GOV.UK provides guidance on their construction, and must never be shared. All applications used by FS must have passwords and wherever possible two-factor authentication applied.

Remote Access Policy

4.16 SunSystems – the finance software used by FS – is server based and accessible via remote access. Remote access permission must be approved by FS [in practice the CFOO] and set up by Microsys.

Removable Media

4.17 The use of flash drives should be minimised. If used, they must be password protected.

Server Security

4.18 All FS's systems are cloud based with the exception of SunSystems which is server based. The configuration of the server is undertaken by Microsys who are also responsible for deploying updates and patches as required.

Software Installation

4.19 To reduce the risk of viruses and malware, software can only be installed on FS devices with the approval of FS [in practice the CFOO] and must be installed by Microsys.

Technology Disposal

4.20 All FS IT equipment must be returned to the CFOO when it is no longer required or when an employee leaves the organisation. If equipment is found to be defective or end of life it will be transferred to Microsys for secure disposal to ensure all FS information is completely removed.

User Access

4.21 FS wishes to operate in the most transparent manner possible. It has an agreed folder access policy for staff with only information on Finance [payroll], SMT workings, and Board/ Governance not accessible to all staff. In practice most communications / decisions arising from work undertaken by the SMT and Board are shared with staff via updates.

4.22 SharePoint is accessible by FS Board and Committee members, Microsys and Gravitate HR. These groups may also have access to other FS Software as required – for example RiskMate – our Risk and Incident Management System.

4.23 Upon leaving FS's employment, ex-employees will have access to all systems removed. It is the responsibility of the CFOO to liaise with Microsys to ensure this is undertaken on the last day of employment.

Wireless Usage

4.24 FS employees are home based and may also make use of workspaces outside of their home [such as Hubs] therefore wireless connectivity is assumed. However, insecure wireless networks can make IT systems vulnerable to malicious attacks. Only secure wireless connections should be used. When making use of a wireless network in the home, FS requires employees to change the default supplied router login and password.

5 Roles and Responsibilities

5.1 All those mentioned in 2.1 have a responsibility to ensure compliance with the GDPR and this policy, and to develop and encourage good information handling practices.

6 Training

- FS Induction T001 - Keeping our Information Secure
- FS Induction T002 - An introduction to GDPR
- LMS - Data Protection
- LMS - Understanding Cyber Security
- LMS - GDPR
- LMS - IT security for the Remote Worker and Business Traveller

7 References

- The Computer Misuse Act (1990)
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)

8 Review

8.1 This policy is reviewed, approved, and endorsed by the Board of trustees. It is updated when required by legislation, to ensure that it reflects statutory responsibilities, government guidance and best practice for FS, or every 24 months whichever is the soonest.