Data Security Policy

Measures to keep information secure

Author: Russell Cosway (Gydeline)

Owner: John Scott (Bees United Membership Secretary)

1 Table of Contents

2 Introduction

2.1 Purpose

Ensure that all technical and organisational systems used by Brentford Football Community Society Ltd (t/a Bees United) are fit for purpose, support the business strategy and do not expose the company or any of its stakeholders to any foreseeable risks.

2.2 Scope

All systems used by directors and others working on Bees United's behalf. Covering company, cloud and some aspects of personally owned ICT. Interfaces to external partners, suppliers and customers are partially in scope.

2.3 Key Principles and Definitions

2.3.1 Roles and Responsibilities

- Accountable Person (owner) - Define and seek approval of this policy, ensure all are familiar with responsibilities and procedures (see statement 3)
- Technology Director – primary contact and responsible for ensuring all technological measures are specified, implemented, maintained and monitored. John Scott is the Technology Director at time of approval.
- Information Director – responsible for all data protection, data privacy and information management matters and ensuring defined organisational measures are followed to support the technical measures. John Scott is Information Director at time of approval
- All Directors - Understand the policies and ensure procedures are followed and data is protected
- Workers (which includes directors) – Understand reasons for security measures and the consequences of not following process and procedure correctly and consistently

2.3.2 Applicable Regulations & Standards

- Data Protection Act (GDPR)
- Privacy and Electronic Communications Regulations
- National Cyber Security Centre – Cyber Essentials
- ISO 27001 – Information Security Management Systems

3 Policy Statements

3.1 General

1. Deliberate or reckless failure to apply policies, process and procedures will result in the application of the **Disciplinary Process**.
2. The Technology Director acts as the Primary Administrator and will appoint, and train, at least one other director to act as an administrator.
3. A 3rd party organisation may be contracted to act as an administrator and/or deliver services to support the security of the organisations information
4. All workers are regularly updated and reminded of the organisations policies and their responsibilities related to achieving and maintaining compliance.
5. Appropriate and timely education, training and guidance is provided to ensure all staff have the required skills, qualifications and resources to provide services to the required standard
6. Collection of data is only made from reliable and reputable sources.
7. Deliberate or reckless failure to apply policies, process and procedures will result in the application of the disciplinary procedure.

3.2 User and Administrative Access

1. All passwords must be strong and meet password standards (see NCSC Password guidance)
2. Wherever available, two factor authentication solutions are used
3. Only authenticated users, created by an administrator have access to the organisations digital resources e.g. file storage)
4. Where possible, systems should be configured to lock user accounts that have failed to log in successfully after 5 attempts. A process to unlock such accounts will be communicated to all users.
5. All user and administrative accounts on devices will be allocated to a known individual, where possible. There should be no anonymous accounts on a device unless they are mandatory.
6. User and administrator accounts are removed or disabled within 24 hours of them no longer being required
7. Elevated privileges are only provided on user accounts following a process to assess the risk and then for only a specified time period.
8. Elevated privileges provided to users are regularly reviewed and removed as soon as they are no long necessary.
9. Administrator accounts will not be used for sending or receiving emails, browsing the internet, accessing untrusted resources (e.g. USB storage device) or accessing business applications.
10. A user may be provided with a separate administrator account with which they can undertake required administrative duties; user accounts will have no administrator privileges.

3.3 Firewalls and Networks

1. There are no Boundary firewalls and should one be required in the future, then this statement will be removed and replaced with ones applicable to administering a private network
2. Any device using the organisations technical resources (e.g. storage) has a firewall installed on the network and devices they are using
3. All firewalls are configured to block unauthenticated connections by default
4. When Wi-Fi connections are utilised is it encrypted using WPA-2 or better.
5. A Virtual Private Network (VPN), or services employing similar encryption solutions, are used whenever viable

3.4 User Devices

1. All devices will be configured, during implementation, to disable automatic execution of any code without the users, ideally an administrators, authorisation (i.e. no autorun)
2. All desktop and laptop computers must have up-to-date anti-malware software installed and configured prior to accessing any of the organisations resources
3. Passwords for required default accounts on software or hardware must be immediately changed prior to implementation

3.5 Software Management

1. All software used on behalf of the organisation is appropriately licensed and is supported and is capable of being patched

3.6 Storage

1. Information stored in cloud storage solutions is encrypted at rest and in transit

3.7 Incidents

1. There is an Information Security Incident Management process which is regularly reviewed and rehearsed
2. An Information Security Incident will be logged if a loss of integrity or confidence in data has actually occurred or is suspected to have occurred
3. Business continuity plans are maintained, rehearsed and tested regularly

3.8 3rd Parties

1. Any person or organisation appointed to work, either under contract or voluntary agreement, is inducted into this policy and any other relevant to their work.

4 Implementation

4.1 Approval and review

This policy has been agreed and adopted by the board on the DATE

A review will be undertaken every 12 months or directly after a Breach.

4.2 Communications

The policy will be communicated as follows:

4.2.1 Externally

- Reflected in Privacy Notice
- Induction of 3rd party workers

4.2.2 Internally

- New director induction process
- Regular director and volunteer training
- Discussion and reminders in meetings

4.3 Accountability

The Bees United Chairperson (Chair) is accountable for ensuring that this policy is fully implemented, followed and audited. Stewart Pervis was Chair at time of approval

5 Document Control

Key Details

Doc Ref.	POL-DataSecurity-D03.docx	Date	6/21/21
Title	Data Security Policy	Owner	Bees United Chair
Status	DRAFT 0.3	Audience	Directors, volunteers, suppliers
Purpose	Measures to keep information secure	Tags	Personal, data, protection, privacy

Version History

Version	Date	Author	Details
D01	25/5/21	Russell Cosway	Initial Draft
D02	17/6/21	Russell Cosway	Refinements to role holders
D03	23/6/21	Russell Cosway	Reinstated content following save error
V01			

Approval

Name	Role	Job title	Contact Details
Stewart Purvis	Approver	Chair	name@company.com
John Scott	Responsible	Technology Director	name@company.com

6 Bibliography

End of Document

Produced: 01/02/2023 13:53:00

Gydeline Ltd is a company limited by shares, registered in England and Wales with Companies House, No. 09559617

Registered Office: North Wing, Norway House, Summers Street, Lostwithiel, Cornwall, PL22 0PT

VAT No: GB 226 0817 24

Telephone: 03330 095260 hello@gydeline.com www.gydeline.com