Normandy Community Shop and Café Ltd
GDPR Policy

1. Introduction

The Normandy Community Shop and Café Ltd, hereafter known as 'the Shop' or 'the Society', a registered society under the Co-operative and Community Benefit Societies Act 2014 and owned by its members, the majority of whom are residents of the village of Normandy. The Society operates from the Shop site within Normandy village, just outside of the Surrey Hills Area of Outstanding Natural Beauty and delivers various services for the benefit of residents of Normandy, the wider area and visitors to the village. The Shop is a socially responsible business committed to commercial success whilst upholding the highest standards with regards to business operations. This policy forms part of those standards of good practice.

The Shop collects and administers a range of personal information for the purposes of employing staff, maintaining our register of members and in our function as a shop for Normandy, as well as for the purposes of marketing and publicity. The Shop is committed to protecting the privacy of personal information it collects, holds and administers.

2. General Policy Statement

We are fully committed to comply with the requirements of the General Data Protection Regulation and the Data Protection Bill ('the Act').

We adhere to the principles which underline the Act, namely that all data which is covered by the Act (which includes not only computer data, but also personal data held within a filing system) is:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) accurate and, where necessary, kept up to date.

(e) kept in a form which permits identification of data subjects for no longer than is necessary.

(f) processed in a manner that ensures appropriate security of the personal data.

The Shop has adopted the following principles contained as minimum standards in relation to handling personal information.

The Shop will:

- Collect only information for which the organisation has a legal basis.

- Ensure that stakeholders are informed as to why we collect the information and how we administer the information gathered;
- Use and disclose personal information only for our primary functions or a directly related purpose, or for another purpose with the person's consent;
- Store personal information securely, protecting it from unauthorised access; and
- Provide stakeholders with access to their own information, and the right to seek its correction.

3. DATA PROTECTION POLICY

3.1. Responsibilities

The Company Secretary is responsible for:

- ensuring that the Shop is registered with the Information Commissioner's Office & registration is renewed annually
- the details of the Shop as registered are kept up to date & reviewed annually

The Shop maintains this policy for monitoring changes in Privacy legislation, and for advising on the need to review or revise this policy as and when the need arises.

All staff are trained on Data Protection compliance on induction and receive updates as required including any changes to this policy and refresher training.

Staff are individually responsible for ensuring that they do not commit any breaches of this policy. Breach of the policy may result in disciplinary action.

Each staff member is responsible for reporting any breach, or suspected breach of this policy to the Company Secretary who will conduct an incident management plan in accordance with our Information Management and Security Policy.

The Legal Sub-Committee undertakes an annual review of this policy to verify that the policy is effective and reports to the Management Committee who will adopt the new policy as appropriate

Enquiries about the handling and processing of personal data should be referred to the Company Secretary who is responsible for data protection.

Collection

At the Shop we hold extremely sensitive and valuable information which must be kept safe failing which there could be serious repercussions for members and staff, other individuals as well as for the Shop.

Our policy is to protect the information we hold from all threats, whether internal, external, deliberate or accidental.

It is our policy to ensure that:

- information is protected against unauthorised access;
- information is kept confidential;
- the integrity of information we hold is maintained;
- information is only kept as long as is necessary
- regulatory and legislative requirements are met;
- all breaches of information security, actual or suspected are reported and investigated; and
- business and individual requirements for the availability of information and information systems are met.

We maintain the security and confidentiality of the information we hold as well as our information systems and applications by ensuring that all staff are aware of and fully comply with all relevant UK and European legislation including, but not limited to,:

- the General Data Protection Regulation and the Data Protection Bill;
- the Data Protection (Processing of Sensitive Personal Data) Order 2000;
- The Copyright, Designs and Patents Act 1988;
- The Computer Misuse Act 1990;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000

- having a consistent approach to security by ensuring that all staff are aware of the information security policies and procedures applicable in their work area and fully understand their own responsibilities;
- creating and maintaining within t a level of awareness of the need for information security and data management as an integral part of our day to day business;
- having in place up to date contingency and recovery plans;
- having in place measures to ensure data is secured against loss and unauthorised access;
- protecting the information assets under our control.

3.2 Use and Disclosure

The Shop will:

- Only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose
- For other uses, we will obtain consent from the affected person.

3.3 Data Quality

The Shop will:

- Take reasonable steps to ensure the information the organisation collects is accurate, complete, up to date, and relevant to the functions we perform.

3.4 Data Security and Retention

The Shop will:

- Safeguard the information we collect and store against misuse, loss, unauthorised access and modification.
- Data will not be retained longer than necessary.

3.5 Openness

The Shop will:

- Ensure stakeholders, including our employees, are aware of our Data Protection Policy and its purposes.
- Make this information freely available in relevant publications and on the organisation's website.

3.6 Access and Correction

The Shop will:

- Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date.
- Individuals who wish all data to be personal data to be removed & deleted from the Shop records have the right to do so.

3.7 Anonymity

The Shop will:

- Give stakeholders the option of not identifying themselves when completing evaluation forms or opinion surveys.

3.8 Making information available to other organisations

The Shop:

- Will only release personal information about a person with that person's express permission. For personal information to be released, the person concerned must send permission in writing.
- Will not release information to third parties where it is requested by the person concerned UNLESS required by law to do so.

3.9 Information Assets

We annually assess all of our assets to ensure that appropriate procedures are in place to mitigate the risks. This process is the responsibility of the Legal Sub-Committee.

The register below lists the societies key information assets and identifies the risks to these assets, their likelihood and impact and how we ensure they are protected

Asset	Risk	Likelihood	Impact	Security Measures
Business plan	Low	Low	High	On the Shop web site, Three Rings and in Dropbox
Business Continuity Plan	Low	Low	High	Not yet written
Financial information	Medium	Medium	High	All information kept in Dropbox and restricted to Directors
Accounts information	Medium	Medium	High	Maintained on Xero and in the office storage. Access only Directors and Gen Mgr & accountants. Copies of accounts information held by external accountants.
Staff records inc Volunteers	Medium	Medium	High	All information kept locked in the office storage, and Three Rings with access restricted to Gen Mgr & Directors.

Complaints information	Low	Low	High	Complaints information kept locked in office storage & on Dropbox . Access restricted to Directors.
Money laundering disclosures- check for PO	Low	Low	High	All information kept in Dropbox and restricted to Directors
Members/Shareholder details	Medium	Medium	High	These documents are kept in the relevant file and stored securely in locked cabinets. On digital files they are secure on the Three Rings & backed up on Dropbox
Board minutes and papers	Medium	Medium	High	These documents are kept in the relevant file and stored securely in locked cabinets and Three Rings
Customer info	Low	Low	Low	Information held in EPOS and Three Rings with restricted access
CCTV System	Low	Low	Low	Not yet installed
Suppliers	Medium	Low	Medium	Supplier contact detail held in Three Rings

27.5 Access controls

Drop box - the administrator is a nominated Director. S/he is responsible for creating access to the Directors documents.

Xero – the administrator is a nominated Director

Office passcode. This will be re-set from time to time and notified to the Directors and key users.

Access rights will not be provided/amended without the prior authentication and authorisation by the nominated Director.

Requests for new accounts or requests by existing users for amendments or adjustments to access rights must be made to the nominated Director.

Any limits on access will be confirmed to the user prior to authorisation. Staff members' user rights generally cease upon termination of their employment contract or in the case of volunteers informing the Gen Mgr of their intention to leave..

User accounts shall only be used by the person (or persons) it was issued to. Each user is responsible for the appropriate use of their accounts in accordance with our IT Policy.

27.6 Destruction of data

The following procedures set out how long information will normally be held by us and when that information will be confidentially destroyed.

Retention Periods

The storage of data will be restricted to that needed for a legitimate business reason.

Unless expressly stipulated otherwise by the Directors, records will ordinarily be kept for at least the following periods:

Shareholder Information	
Information	**Retention Period**
Shareholder details	12 months after the shareholder has withdrawn their shares.
Shareholder Complaints	6 months after the complaint has been concluded.
Staff Information	
Information	**Retention Period**
Application forms/interview notes for unsuccessful candidates	12 months
Offer letters and acceptance	9 months after employment ceases
Disciplinary, working time and training	9 months after employment ceases
Redundancy details	9 months from date of redundancy
Documents proving the right to work in the UK	Two years after employment ceases
Health and safety/EHO reports	Permanently
PAYE Records	4 years

Workplace accidents	3 years after date of last entry. There are specific rules on recording incidents involving hazardous substances
Payroll	3 years after the end of the tax year they relate to
Statutory maternity, adoption and paternity pay	3 years after the end of the tax year they relate to
Statutory sick pay	3 years after the end of the tax year they relate to
Working time arrangements	2 years from date on which they were made
Corporate Information	
Information	**Retention Period**
[Directors/Members] Meeting Agendas, Reports and Minutes	Permanently for historical purposes
Constitutional documents, Resolutions and Special Resolutions	Permanently
Business/Strategic Plans	3 years
Financial Information	
Information	**Retention Period**
Books of account, reconciliations, bills, bank statements and passbooks	6 years
Paid cheques, digital images of paid cheques and other authorities for the withdrawal of money from a client account	2 years
Other vouchers and internal expenditure authorisation documents relating directly to entries to the client account books	2 years
Cardholder data	Unless there is a business need to retain it, cardholder data should be destroyed immediately after the transaction is processed. If cardholder data needs to be retained then it must be destroyed as soon as it is no longer required