Contents

[Goal of the data protection policy 2](#_Toc76759283)

[Scope 2](#_Toc76759284)

[Guidelines. 3](#_Toc76759285)

[Objective 3](#_Toc76759286)

[Definitions 3](#_Toc76759287)

[Roles and Responsibilities 3](#_Toc76759288)

[Security policy and responsibilities in the company 4](#_Toc76759289)

[Policy Statement 4](#_Toc76759290)

[Implementation 6](#_Toc76759291)

[Data Protection Regulator: the ICO 6](#_Toc76759292)

## Goal of the data protection policy

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) and Data protection Act (DPA) 2018 but also to provide proof of compliance.

## Scope

The Data Protection Policy (the Policy) ensures the The General Store Selkirk complies with Data Protection Law, namely the UK General Data Protection Regulation (UK GDPR) and the [Data Protection Act (DPA) 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted). These set out the framework for how the UK processes personal data:

* UK GDPR, enforceable in all EU member states from 01 January 2021, covers most of the legal obligations for processing personal data in the UK. DPA enacts UK GDPR and replaces the DPA 1998. It sets out:
* how other information rights legislation (e.g. Freedom of Information Act 2000) interact with the new DPA and UK GDPR
* how personal data must be processed in the UK where it doesn't fall within UK GDPR, e.g. immigration or national security matters
* local rules for the UK that complement UK GDPR, e.g. additional measures required for the processing of special category personal data
* the Information Commissioner’s Office’s (ICO) role, functions and powers.

The Policy applies to:

* *All staff (employed and contracted), and suppliers* who handle and use our information (where we’re the 'Controller' for the personal data being processed), whether we hold it on our systems (manual and automated) or if others hold it on their systems for us
* *All personal data processing* we carry out for others (where we’re the 'Processor' for the personal data being processed)
* *All formats*, e.g. printed and digital information, text and images, documents and records, data and audio recordings.

## Guidelines.

In order to conduct its normal business, The General Store Selkirk, collects and uses certain types of personal information about living individuals. This is collected from staff, volunteers, suppliers, customers and makers submitting items to sell in the retail section.

The type of information collected includes and is not limited to Names, addresses, contact numbers, email addresses, suppliers and all other with whom it has business or communicates.

## Objective

Our objective in this policy is to comply with the Data Protection law, meet the standards set out, proctect the rights of all involved with The General Store Selkirk and protect The General Store Selkirk from risks of a data protection breach.

## Definitions

“*Personal Data*” is all information that relates to an identifiable living person (or “Data Subject”) **and** that can be used to identify the person directly, or indirectly when used with other information

*“Processing”* relates to all actions or handling of personal data by manual or automated means, e.g. data collection, erasure and destruction plus everything in between including recording, use, disclosure, sharing and storage.

## Roles and Responsibilities

* The UK GDPR applies to ‘controllers ’*and* ‘processors’.
* A controller determines the purposes and means of processing personal data.
* A processor is responsible for processing personal data on behalf of a controller.

The General Store Selkirk is predominately a ‘data controller’ when processing personal data, eg When we provide a service such as a repair to an item, we collect personal data in order to facilitate the end result of returning the item in a repaired state.

The General Store Selkirk is sometimes a ‘data processor’ as we pass data to other services outside our organisation to carry out a repair.

## Security policy and responsibilities in the company

*Staff* must understand, keep up-to-date with, and comply with the Policy Line managers’ must apply the Policy across their team(s) cascade data protection awareness communications to staff making sure they comply with the Policy.

*Directors/Managers* must apply the Policy across their team(s) cascade data protection awareness communications to their team(s) make sure their staff comply with the Policy make sure their staff complete the mandatory Data Security Awareness training within given timescales monitor suppliers and partners' compliance with the Policy through routine procurement and contract management activities, e.g. use appropriate contractual clauses and supporting information sharing agreements.

*Directors, Staff, Volunteers, Trainees, representatives and suppliers* must follow all the data protection requirements in their respective role descriptions, contracts, terms and conditions and/or Code of Conduct.

## Policy Statement

The General Store Selkirk commits to processing all personal data in compliance with the *data protection principles* (unless a data protection law exemption applies). Personal data must:

* Be processed lawfully, fairly and in a transparent manner (*Lawful, fair and transparent*)
* Be obtained only for specific, lawful purposes (*Purpose limitation*)
* Be adequate, relevant and limited to what is necessary (*Data minimisation)*
* Be accurate and, where necessary, kept up to date (*Accuracy*)
* Not be held for any longer than necessary (*Storage limitation*)
* Be protected in appropriate ways (*Integrity and confidentiality/Security*)

The General Store Selkirk must demonstrate how we comply with the above principles this is inclusive of but not limited to Data Protection Policy, Absence and Sickness Policy, Disciplinary Policy, Equality, Diversity and Inclusion Policy, Dismissal Policy.

All personal data processing must have a *lawful basis for processing*from the following:

* the Data Subject *consents* to the processing of their personal data
* the processing is necessary:
  + to enter into or carry out a *contract* with the Data Subject, for activity such as a repair
  + to comply with our (or another Controller’s) *legal obligations*
  + to protect the *vital interests* of the Data Subject
  + to exercise our (or another Controller’s) official authority or perform a *public interest task*
  + to meet the *legitimate interests* of a Controller or another third party.

Of these lawful bases, the The General Store Selkirk most frequently uses the following which then determine which of The General Store Selkirks procedures and ways of working must be adopted:

* *contract* – where this applies,
* Repair information, the contracts must be written in the appropriate ledger
* be kept safe from public scrutiny
* be up-to-date.
* *legitimate interests* – where this applies, the Data Subject must be notified.
* *consent* – where this applies, the Data Subject must provide explicit and informed consent for example when passing information to a third party maker.

The General Store Selkirk commits to the processing of all personal data in compliance with the Data Subjects’*Individual Rights*(unless a data protection law exemption applies).

Data Subjects have:

1. the right to be *informed* - e.g. Fair processing/privacy notices
2. the right of *access* - e.g. subject access requests (SARs)
3. the right to *rectification* - e.g. have their data corrected
4. the right to *erasure* – e.g. have their data deleted/removed
5. the right to *restrict processing* – e.g. stop their data being used
6. the right to *data portability* – e.g. transfer their data easily
7. the right to *object*– e.g. challenge what we’re doing with their data
8. rights in relation to *automated decision making and profiling* – e.g. safeguards to make sure we don’t make potentially damaging decisions about them without human involvement.

As part of these rights, Data Subjects can:

* make a verbal request against any of the rights listed above
* complain to the ICO about data protection breaches and can bring court proceedings for compensation where a data protection breach has caused them damage (including distress).

## Implementation

*In summary:*

* All staff must receive*training*, appropriate to their role, to help them understand how to process personal data in line with the Policy - e.g. complete the annual, mandatory data security awareness training and other training as and when required, such as Privacy and Consent (includes marketing consent), Data Protection Impact Assessments and Information Sharing. Please see the current Learning and Development Programme for details of scheduled sessions
* All staff must assess and *manage the risks* around how they process personal data to make sure it’s *classified and handled* appropriately.
* All *‚The General Store Selkirk***‘** staff, representatives and suppliers must follow all the data protection requirements in their respective role descriptions, contracts, terms and conditions and/or Code of Conduct
* All staff must inform the IG Officer (a Director – TBA) of any Individual Rights Request received relating to the The General Store Selkirk
* All staff must promptly report potential or actual *breaches* of the Policy or data protection law to the IG Officer
* All staff must fully co-operate with any investigation, audit or enforcement activity undertaken by the ICO.
* We will take appropriate action against staff, officer, trainee, member, representative or suppliers found breaching the Policy where appropriate to them. Such action may include but not be limited to disciplinary investigations, dismissal, civil or criminal proceedings and fines.

## Data Protection Regulator: the ICO

The Information Commissioner’s Office (ICO) is the UK's independent body set up to uphold information rights. Find out more about their organisation and structure on their website: <https://www.ico.org.uk>

Helpline Number 0303 123 1113