

Shrewsbury Drapers Holy Cross Ltd Data Protection Policy

Introduction:

The purpose of this policy is to enable Shrewsbury Drapers Holy Cross Ltd (SDHC Ltd 1132671) incorporating Shrewsbury Drapers Company Charity (SDCC 1132671-1) to comply with the law (The GDPR and DPA 2018) in respect of the data it holds about individuals.

Any reference to SDHC Ltd also applies to SDCC if relevant. SDCC is the registered provider of social housing.

SDHC Ltd will ensure that the information the charity holds about its residents, beneficiaries, employees etc. is used in accordance with the law. The charity will only collect and use personal data in compliance with this Policy and the Rules set out below.

The Charity will:

- follow good practice
- protect residents, directors/trustees, staff, volunteers and other individuals by respecting their rights
- demonstrate an open and honest approach to personal data and
- protect the charity from the consequences of a breach of its responsibilities.

This policy applies to all the information that we control and process relating to identifiable, living individuals including contact details, bank details, photographs, audio and digital recording.

SDHC Ltd will comply with General Data Protection Regulations 2018 as follows:

1. **Transparency:** The charity will be open and transparent in the way personal data is used and shared. There may be limited circumstances where the charity does not have to comply with the transparency requirement but in such instances the charity will obtain further advice from the ICO. Individuals will be provided with information about how their personal data is collected and stored.
2. **Collecting and Using Personal Data for Lawful purpose only.** The charity will only collect and use the minimum amount of personal data if relevant for the purpose of the charity and where the charity can rely on a lawful basis (or bases) and where the purposes have been identified in a privacy notice provided to individuals, for example in the charity's application form. When collecting personal data from individuals the charity will ensure that the individuals are aware of the purposes for which the personal data will be used.

In addition, when collecting personal data, the charity will only collect those details which are necessary for the purposes for which that personal data is being obtained. Any use of personal data will be for the identified purposes and any different or new purposes will have a lawful basis. Personal data that is not necessary for any legitimate business purpose will not be collected or accessed.

SDHC Ltd has identified that the charity has a legitimate interest in keeping personal data about residents as directors/trustees must be satisfied that each resident qualifies as a beneficiary of the charity in accordance with the

Memorandum of Association and Articles of Association dated 11 February 2015 and the Scheme for SDCC dated 31 December 2014 .

The charity considers the processing and storing of such personal data is necessary to comply with the Governing Document. All personal data, including details of residents' next of kin, will be stored securely, data on computer will be password protected and paper copies of data will be kept in a locked filing cabinet. Only authorised members of staff and directors/trustees will have access to personal data.

3. **Privacy Impact Assessments and Privacy by Design.** The directors/trustees consider that the use of personal data is unlikely to result in significant risks for the rights and freedoms of individuals and therefore a Privacy Impact assessment is not necessary. The charity will ensure that systems, databases and tools that collect and use personal data are designed to promote privacy protection.
4. **Ensuring data quality.** Processing inaccurate information can be harmful to individuals and the Charity. The main way of ensuring that personal data is kept accurate and up to date is by ensuring that the sources the charity uses to obtain personal data are reliable. Individuals will be actively encouraged to inform the charity should their personal data change.

To ensure that personal data is accurate, it will generally be collected directly from individuals. All residents will be actively encouraged to update their contact details by notifying the charity of any changes in their personal data.

5. **Retaining and disposing of data.** Any personal data must only be kept where there is a business or legal need to do so. When the charity disposes of personal data, this will be undertaken in a secure manner.

Documents (including paper and electronic versions and email) containing personal data will not be kept indefinitely and will always be securely deleted and destroyed once they have become obsolete or when that personal data is no longer required. Paper based documents will be shredded on site or disposed of externally as confidential waste. Electronic data will be permanently deleted from all drives and electronic media. Computer equipment that is surplus to requirements will be disposed of securely by specialist contractors. The charity will maintain a record of the details of the media and computer equipment that has been disposed of, when it was disposed of and how it was disposed of and by whom.

Personal data will not be retained simply on the basis that it might come in useful one day without any clear view of when or why.

The charity's data retention policy is:

In particular, the Charity will not keep personal data for longer than is necessary. In addition to personal data other documents are held for defined periods of time. A comprehensive list is given below:

Insurance Policies	3 years
Employers Liability Insurance Certificate	40 years
Accident reports and documents	6 years
Trustee/Director meeting minutes	10 years minimum
General meeting minutes	10 years minimum

Annual accounts	permanent
Health and safety records	6 years Permanent for hazardous substances
Contracts, guarantees and licensing agreements	6 years after expiry
Buildings plans and warranties	permanent
Health and safety files	permanent
Employee applications and interview notes	6 months-1 year
Maternity Pay records and certificates	3 years after tax year when maternity ends
Sick pay records and certificates	3 years after tax year
Names of residents and dates of occupancy	Permanent
Resident files and correspondence	6 years after leaving/ death
Records of complaint and investigations (resident)	6 years
Charity documents containing sensitive data held by any trustee	1 year after receipt unless still relevant including all computer data and paper copies
Names of trustees/directors and dates of positions held	Permanent
Trustees personal files	6 years after ceasing to be a trustee
Resident meeting minutes	1 year
Employee staff meetings minutes	1 year
Water temperature logs	1 year
Payroll documentation	6 years
Employee accident books	6 years
Organisation charts	permanent
Wages and salary records, redundancy, expenses	6 years
Timesheets/ working hours	2 years
Staff personal files	6 years after employment ceases
Resident applications which are refused/ withdrawn	1 year

6. **Honouring Individuals' rights.** The charity will reply to queries and complaints from individuals about how the charity uses their personal data within 30 days.

Individuals are entitled by law (by making a request) to be supplied with a copy of any personal data held about them (including both electronic and paper records). Individuals are also entitled to know the logic involved in decisions made about them.

An individual also has the right to seek erasure of their data and to request portability of their data i.e. that the charity provides their data to them in a structured, commonly used and machine-readable format.

Where the charity receives a request from an individual exercising their legal right to control their personal data, the charity will respond promptly. If a valid request concerns a change in that individual's personal data, such information will be rectified or updated, if appropriate to do so.

7. **Taking appropriate security measures.** Personal data will be kept secure. Technical, organisational, physical and administrative security measures (both computer system and non-computer system related steps) are necessary to prevent the unauthorised or

unlawful processing or disclosure of personal data, and the accidental loss, destruction of, or damage to personal data.

The charity will monitor the level of security applied to personal data and take into account current standards and practices. As a minimum the charity will ensure that:

- Personal files for residents, directors/trustees, and employees are kept in a locked filing cabinet at all times with access only by authorised staff.
- Applications for accommodation are kept in a locked filing cabinet at all times with access only by authorised staff.
- Trustee's details are kept in a locked filing cabinet with access only by the Company Secretary or deputy.
- Electronic files containing personal data are password protected and passwords will be changed on a regular basis.
- Backed up electronic data is held securely on an alternative site or when off-site it is encrypted, password protected and will only be accessed by named staff.
- If any personal data is taken from the office (e.g. to work at home) the personal data will be held securely at all times whilst in transit and at the location where held.

Any suspicion of any data security breach should be reported immediately to the Data Controller. When the charity becomes aware of a breach, protective measures will be taken to effectively mitigate the consequences of the breach.

8. **Using Subcontractors and Vendors.** Under EU data protection law, where a provider of a service has access to personal data (e.g. as a payroll provider) the charity will impose strict contractual obligations dealing with the purposes and ways personal data may be used and the data security of that information. These are third parties who act as processors (i.e. only holding the personal data according to the charity's instructions) and this will include telecare companies that provide services to the charity (Housing Benefit and Government offices are not vendors).

The charity will carry out appropriate due diligence on any potential third party to which personal data is being provided and ensure that the third party's Data Privacy Policy is adequate.

The charity will always enter into a written contract with any Vendor that deals with personal data being provided by the charity. The contract will meet the requirements under the GDPR Article 28.

9. **Disclosure to Third parties.** At times, the charity may disclose personal data to vendors, contractors, service providers and other selected third parties. This is very unlikely to happen apart from an emergency situation where the health or security of an individual is endangered.

Prior to disclosing personal data to these parties, the charity will take reasonable steps to ensure that: (i) the disclosure of personal data is appropriate; (ii) the recipient of such information is identified; and (iii) where appropriate or required by law, the third party is contractually committed to complying with this Policy and/ or the charity's instructions concerning the use of personal data as the charity well as implementing appropriate security measures to protect personal data, limiting further use of personal data, and complying with applicable laws.

In certain circumstances, the charity may be required to disclose personal data to third parties when required by law, when necessary to protect the charity's legal rights, or in an emergency situation where the health or security of an individual is endangered. Prior to such disclosures, the charity will take steps to confirm that the personal data is disclosed

only to authorised parties and that the disclosure is in accordance with this Policy and applicable law.

10. **Safeguarding the use of special categories of data.** Special categories of data is information revealing an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, processing of genetic data or biometric data (for the purpose of uniquely identifying an individual), health and sex life or sexual orientation. Since this information is more intrusive, the charity will only use it where absolutely necessary and often with the explicit consent of the individual affected.

The charity will only hold and make available special categories of data on an individual without their explicit consent if the charity have another lawful basis under applicable law. This may be the case, for example, where the charity holds information about an individual's health where this is necessary to exercise any obligation conferred by law on us in connection with the charity.

For residents and beneficiaries the charity may also collect and use their special category data where:

- Our use of their personal data is to provide support for a particular disability or medical condition
- Our use of their personal data is necessary for providing confidential counselling, advice or support
- Our use of their personal data is necessary for protecting an individual from negligence or physical, mental or emotional harm
- Our use of their personal data is necessary for the purpose of protecting the economic well-being of an individual at economic risk and is of health data

The charity will always assess whether special categories of data are essential for the proposed use and will only collect special categories of data when it is absolutely necessary in the context of the organisation. Application (or other) forms used to collect special categories of data will include suitable and explicit wording expressing the individual's consent when the charity are collecting explicit consent.

Consent must be demonstrable. Therefore, if it is collected verbally it will be recorded in such a form as to prove that the requisite information was provided to the individual and their response was able to be verified.

Where consent is not relied upon, the charity will take steps to ensure that there is another lawful basis under applicable law for the collection and use of such information. In certain circumstances, the charity may be required to consult with the Information Commissioner's Office about the proposed use of such special categories of data.

11. **Collecting Children's Data.** Data pertaining to children will not be collected.

Data Storage and processing:

SDHCLtd recognises that data is held about:

- residents
- directors/trustees
- staff
- volunteers
- members.

This information is always stored securely and access is restricted to those who have a legitimate need to know. We are committed to ensuring that those about whom we store data understand how and why we keep that data and who may have access to it. We do not transfer data to third parties without the express consent of the individual concerned.

Archived records are stored securely and the charity has clear guidelines for the retention of information as set out in Point 5 above.

Rights of individuals

All individuals who come into contact with SDHC Ltd have the following rights under the DPA:

- a right of access to a copy of their personal data
- a right to object to processing that is likely to cause or is causing damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed and
- a right to claim compensation for damages caused by a breach of the DPA.

The directors/trustees recognise their overall responsibility for ensuring that the charity complies with its legal obligations. The designated Data Protection Officer is responsible as follows:

Roles and Responsibilities:

- briefing directors/trustees on Data Protection responsibilities
- reviewing Data Protection and related policies
- advising other staff on Data Protection issues
- ensuring that Data Protection induction and training takes place
- notification
- handling subject access requests.

All directors/trustees, staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their roles.

Significant breaches of these policies will be handled under disciplinary procedures.

Key risks to the safety of data control and process:

The directors/trustees have identified the following potential key risks:

- breach of confidentiality (information being given out inappropriately)
- individuals being insufficiently informed about the use of their data
- misuse of personal information by staff or volunteers
- failure to up-date records promptly
- poor IT security and
- direct or indirect, inadvertent or deliberate unauthorised access.

The directors/trustees will review the charity's procedures regularly, ensuring that the charity's records remain accurate and consistent and in particular:

- IT systems will be designed, where possible, to encourage and facilitate the entry of accurate data
- data on any individual will be held in as few places as necessary and directors/trustees and staff will be discouraged from establishing unnecessary additional data sets
- effective procedures will be in place so that relevant systems are updated when information about an individual changes.

Subject Access Requests

Any individual who wants to exercise their right to receive a copy of their personal data can do so by making a Subject Access Request ('SAR') to the Data Protection Officer. The request must be made in writing and the individual must satisfy the Data Protection Officer of their identity before receiving access to any information.

A SAR must be answered within 30 calendar days of receipt by the charity.

Collecting and using personal data

SDHCLtd collects and uses personal data in connection solely to meet the objects of the charity. The charity collects personal data mainly in the following ways:

- *by asking applicants for accommodation to complete paper forms*
- *by asking residents to give required personal information to staff verbally*
- *by asking appointees to the Board as Trustees of the Charity and Directors of the Board, such personal information as is required by the relevant regulatory authority (Charity Commission and Companies House.)*

SDHCLtd will:

- not use any of the personal data it collects in ways that have unjustified adverse effects on the individuals concerned
- be transparent about how it intends to use the data and give individuals appropriate privacy notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect
- not do anything unlawful with the data.

Keeping Data Secure

SDHCLtd will take all appropriate measures to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction. This means that:

- *personal files for residents, directors/trustees, and employees and applications for accommodation will be kept in a locked filing cabinet at all times with access only by authorised staff*
- *directors/trustees' details will be kept in a locked filing cabinet with access only by the Company Secretary*
- *electronic files containing personal data will be password protected and passwords will be changed on a regular basis*
- *backed up electronic data will be held securely on an alternative site or when off-site it will be encrypted, password protected and only accessed by named staff*

- *if any data is taken from the office (e.g. to work at home) the data must be held securely at all times whilst in transit and at the location the data is held.*

More information:

Full information about the Data Protection Act, its principles and definitions can be found at www.ico.org.uk

Prepared July 2018