SALVATION ARMY TRADING COMPANY

Data Protection Policy

Author: John Woods, Head of Projects
Date: April 18

Data Protection Policy

Version History and Control Sheet

Document Title	Data Protection Policy
Version	3.0
Date of Original Creation	August 2015
Date of Last Issue	N/A
Author/s	John Woods
File Name	Data Protection Policy

Document History			
Version Number	**Purpose/ Change Details**	**Author**	**Date**
0.1	Original drafted document	John Woods	June 15
1.0	Feedback	John Woods	June-15
2.0	Published	John Woods	August-15
3.00	Updated GDPR	John Woods	April -18

Document Sign Off			
	Signature	Name	Date
Managing Director	*Trevor Caffull*	Trevor Caffull	30/4/18
Projects Manager	*John Woods*	John Woods	30/4/18
Head of IT/DPO	*Ian Barrett*	Ian Barrett	30/4/18

Data Protection Policy

Contents

Data Protection Policy

1. Introduction

SATCoL needs to gather and use certain information about individuals and volunteers.

These can include customers, suppliers, business contacts, employee's, volunteers and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

The definition **"Personal data"** applies to all data that the company holds relating to individuals no matter the method of contact face to face/mail/telephone/Websites.

2. Why this policy exists

This Data Protection Policy ensures SATCoL:

- Complies with Data protection laws including the General Data Protection Regulation (GDPR) and follows good practice
- Protects the rights of staff, customers and others
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach and takes appropriate action
- Undertakes Regular Reviews of processes involving personal data and documentation updated accordingly

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports; and
- records of personal data breaches.

3. Policy Statement

SATCoL not only intends to comply with its obligations under the Data Protection Act 1998 and GDPR, but also assures both employees and all other persons about whom it retains personal data, that this will be processed in compliance with the legislation and any Codes of Practice issued by the Information Commissioner .Data will be stored in a secure, confidential and appropriate manner.
Data Protection guidance and training is made available to assist staff in complying with this policy.

The data will only be stored whilst relevant and will not be disclosed to any person without the data subject's personal written authority or unless required by law.

Under Articles 5 & 16 of the GDPR individuals have the right to have inaccurate personal data rectified. SATCoL will ensure an individual may be able to have incomplete personal data corrected and updated.

4. Data Protection Law

The Data Protection Act 1998 describes how organisations – including SATCoL – must collect store and handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Be processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA) , unless that country or territory also ensures an adequate level of protection

Additionally the following Individual's Rights as described by GDPR are adopted

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

- If we are a controller for personal data we process, we document all the applicable information under Article 30(1) of the GDPR.
- If we are a processor for the personal data we process, we document all applicable information under Article 30(2) of the GDPR.

We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice

People, risk and responsibilities

5. Policy Scope

This policy applies to:

- The Wellingborough Support Centre of SATCoL
- All retail outlets and processing centres of SATCoL and its operating divisions
- All staff and volunteers of SATCoL
- All contractors, suppliers and other people working on behalf of SATCoL

The definition **"Personal data"** applies to all data that the company holds relating to individuals, even if that information technically falls outside the Data Protection Act 1998. This can include:

- Names of individuals
- Postal Addresses
- E Mail addresses
- Telephone numbers
- Any other information relating to individuals

7. Accountability and Governance

Satcol will

- implement appropriate technical and organisational measures that ensure compliance. This will include internal data protection schedules including staff training, internal audits of processing activities, and reviews of internal HR policies, chart of data
- maintain relevant documentation on processing activities;
- appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default.
- create and improve security features on an ongoing basis.
- use data protection impact assessments where appropriate.

8. Data Protection Risks

This policy helps to protect SATCoL from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.
- **Transfer of Data** .For instance when moving data both internally and externally

9. Responsibilities

Everyone who works for or with SATCoL has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
However, these people have key areas of responsibility:

The Senior Management Board (SMB) is ultimately responsible for:

- Keeping the Board of Director's updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone covered by this policy
- Dealing with requests from individuals to see the data SATCoL holds about them (also called subject access requests)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The Head of IT is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the company is considering using to store or process data. For instance cloud computing or remote access to data

The Marketing Manager is responsible for:

- Approving any data protection statements attached to communications such as e mails and letters
- Addressing any data protection queries from media outlets or the press
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

The HR Team is responsible for::

- Ensuring all HR systems, services and equipment used for storing data meet acceptable security standards
- Ensuring sensitive personal information on staff and volunteers records is kept secure
- Ensuring employee and volunteer requests to see and have a copy of personal information held by SATCoL are responded to

10. General staff guidelines

- The only people able to access data covered by this policy should be those **who need it for their work**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers
- SATCoL **will provide training** to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, "**strong" passwords must be used** and they should **never be shared**
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required it should be deleted and disposed of

- Employees **should request help** from their line manager or the data protection officer if they are unsure of any aspect regarding data protection
- Confidential and sensitive data **must never** be shared or linked on social media

11. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IS manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer
- **Data printouts should be shredded** and disposed of securely when no longer required

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees
- If data is **stored on removable media** (like CD or DVD or pen drives) these should be kept locked away securely when not being used. Personal Data may not be stored or moved in this method
- Data should only be stored on **designated drives and servers** and should only be uploaded to approved storage mechanisms
- Servers containing personal data should be **sited in a secure location**, away from general office space
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard back up procedures
- Sensitive and Personal Data should **never be saved directly** to lap tops or other mobile devices like tablets or smart phones
- All servers and computers containing data should be protected by **approved security software and a firewall**

12. Data Use

Personal data is of no value to SATCoL unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by email as this form of communication is not fully secure
- Personal data **should never be transferred outside of the European Economic Area**
- Employees **should not save copies of personal data to their own personal computers**.
- Always access and update the central copy of any data

13. Data Accuracy

The law requires SATCoL to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort SATCoL should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any additional data sets
- Staff should **take every opportunity to ensure data is updated**. For instance confirming a customer's details when they call
- SATCoL will make it easy for data subjects to update the information SATCoL holds about them. For instance by calling our help line,or when ordering on line
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files and postcode comparisons every six months. Requests to remove and update SATCoL records must be made within 28 days of receipt

14. Subject access requests

All individuals who are the subject of personal data held by SATCoL are entitled to:

- Ask **what information** the company holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Be informed how the company is **meeting its data protection obligations**

If an individual or customer contacts the company requesting this information it is called a subject access request.

Subject access requests from individuals should be made by e mail, or in writing addressed to the data controller at data@satcol.org The data controller can supply a standard request form although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant information within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

15 Disclosing data for other reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances SATCoL will disclose the requested data; however the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

14. Providing Information

SATCoL aims to ensure individuals are aware their data is being processed, and that they understand

- How the data is being used
- How to exercise their rights

To these ends the company has a privacy statement setting out how data relating to individuals is used by the company. This is made available on request and is also available on company web sites.

Appendix 1 - Definitions

DEFINITIONS

The following terms are used throughout this policy and its application. These definitions comply with those used within the Data Protection Act. Each term is therefore defined as follows:

"Data" is information which:

- is processed by equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be so processed;
- is recorded as part of a relevant filing system.

"Relevant filing system" means any set of information which is not processed by means of equipment, but is structured in such a way that specific information relating to a particular individual is readily accessible.

“GDPR “ General Data Protection Regulation

"Personal data" is data consisting of information which relates to a living individual who can be identified from that information (or from that and other information) including any expression of opinion about the individual and any indications of the intention of SATCoL or any other person in respect of that individual.

"Sensitive personal data" means personal data consisting of information as to racial or ethnic origins; political, religious or other opinions/beliefs of a similar nature; physical or mental health; sexual life; criminal offences or alleged criminal offences and past sentences; and whether he/she is a member of a trade union.

"Data Subject" is an individual who is the subject of personal data.

"Processing" is obtaining, recording, holding or carrying out any operation on data; such as the organisation, adaptation, alteration, retrieval, disclosure, dissemination, rearranging or destruction of the information or the data.

"Customer or client " is an individual who uses the services of SATCoL .

In addition to the Data Protection Principles being detailed in the SATCoL Policy, these have also been included as an Appendix for ease of reference.

Appendix 2 - Guidelines

GUIDELINES

1. Personal data should only be recorded using either:

Official SATCoL paperwork e.g. application form, or computer systems

Or

Local administrative systems must be approved by the person responsible for your team e.g. Head of Department (for example - local systems are defined as those containing no more than an individual's name, address and contact telephone number.)

(First and Third Data Protection Principles)

2. An individual's personal data must not be disclosed to a third party without consulting and gaining consent from the individual.
(Second Data Protection Principle)

3. All data must be kept factual, clear and precise. Informal notes expressing subjective and unsubstantiated remarks are not acceptable.
(Third, Fourth and Fifth Data Protection Principles)

4. Managers and Team Leaders should retain information for a two year period only, after which time it is archived at Head Office.
(Third, Fourth and Fifth Data Protection Principles)

Retail shops must keep volunteer information for two years on site, or as dictated by HR, after which information must be archived, as advised by your Area Manager

For other SATCoL divisions, the length of time personal information is kept should be agreed with the Division Manager.

5. All personal data must be kept secure at all times
(Seventh Data Protection Principle):-

- Care must be taken to ensure that the security of personal data is not breached by, for example, files being left unattended.
- This particularly applies to information carried by staff when away from office premises.

- Remember to only transport necessary and relevant information.
- Security includes documents in transit i.e. post, fax, photocopier and disc.
- All individuals are responsible for maintaining the confidentiality of their computer passwords and reporting to the IS Department any breach of security immediately.
- To ensure security of computer files staff must adhere to the **IT Do's and Don'ts Guidelines & IT Acceptable Use Policy**
- All home based staff will store personal records in a lockable storage device. Individuals should discuss their requirements with their line manager.
- All Departments should keep personal data in a lockable cabinet or room. Access should be restricted to nominated individuals and keys should be kept in a secure place at all times.
- When files or records are being removed from fixed site premises a record of the individual in possession of the file must be recorded.
- Data should not be removed from its normal place of storage without good reason.

6. Personal information to be destroyed should be shredded.
(Third, Fourth, Fifth and Seventh Data Protection Principles)

7. All requests for access to personal files/records must be made in writing (recommended format Appendix 3).
(Sixth Data Protection Principle)

8. An individual's application to have data corrected or erased must be submitted in writing to the Human Resource Team
Where felt necessary consideration of the application will involve the Data Protection Committee.
(Fourth and Sixth Data Protection Principles)

9. In exceptional circumstances where personal information is to be transferred outside the UK then consultation must take place with the SATCoL Data Protection Controller.
(Eighth Data Protection Principle)

10. Any member of staff who wishes to obtain new personal data must first consult the Data Controller for approval.
(Second and Third Data Protection Principles)

11. Personal data cannot be used for purposes such as conducting questionnaires/surveys or mailing fundraising/marketing literature, without the Individual having given their consent.
(First and Second Data Protection Principle)

The following Individual's Rights as described by GDPR are adopted

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profili

Appendix 3 Access request document

SALVATION ARMY TRADING COMPANY LTD (SATCoL)
SUBJECT ACCESS REQUEST FORM (SAR)
GDPR/DATA PROTECTION ACT 1998

Under the GDPR/Data Protection Act 1998, you are entitled to request access to personal information held about you by Salvation Army Trading Company Ltd. Completing this form will assist us in locating your information quickly and efficiently.

Before completing this form please read the notes at the end of the document

1. Details of the Data Subject

Title (Mr. Mrs. Ms. Other)	
Surname	
First Name(s)	
Date of Birth	
Address (No./Street)	
Address (Town/City)	
Post Code	
Telephone Number	
Email	
Previous address(es)	

2. Are you the Data Subject? (Please tick the appropriate box)
YES If you are the Data Subject, please go to question 5.
NO Are you acting on behalf of the Data Subject with their authority? If so please provide evidence that you are legally authorised to obtain this information, for example, a signed letter of authority.

3. Details of the person requesting the information (if not the Data Subject)

Title (Mr. Mrs. Ms. Other)	
Surname	
First Name(s)	
Date of Birth	
Address (No./Street)	
Address (Town/City)	
Post Code	
Telephone Number	
Email	

4. Please state your relationship with the Data Subject that leads you to make this request for information on their behalf, for example, parent, legal guardian, solicitor.

5. Please help us to narrow down your request by informing use which parts of SATCoL might hold information on you or the data subject. Please tick from the list below the services that you require us to conduct a search on :

• Retail Shops Division	• Clothing Collection Division
• Salvationist Publishing and Supplies	• R Smith & Co/Studio Music
• World of Brass	• World of Sound
• Other – Please specify below e.g. Subscriptions	

6. Documents needed before we can process this application :

   a) Evidence of Data Subject's identify; original proof of identity and address is required to ensure that we only give information to the correct person, for example, a valid photo ID driving licence or passport **and** a recent utility bill, bank statement or Council Tax bill (no photocopies please) showing your name and address. These should be provided by post.

   b) Evidence of the Data Subject's consent, for example, form of authority (if you are making the request on behalf of another);

   c) SATCoL does not charge for processing the subject access request. However However, we may charge a 'reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. Cheques should be made payable to SATCoL .

7. Please read the following declaration carefully, then sign, and date it.

   I ..... certify that the information supplied to SATCoL on this application form is true. I understand that it is necessary for SATCoL to confirm my/Data Subject's identify and it may be necessary to obtain more detailed information in order to locate the correct information.

   Signature : .....

   Date : .....

   Please send your completed form (along with evidence of identify, and address) to:

   SATCoL
   66-78 Denington Road
   WELLINGBOROUGH
   Northants NN8 2QH

   Marked for the attention of the Data Protection Officer

NOTES :

Data Subject : The person that the information is about.

Proof of Identification : The reason we ask for proof of identification is to maintain the security of the information we hold about you. This will help ensure that we do not release your personal information to anybody else. Any documents you send to use will be returned to you.

Previous addresses : If the information you are requesting may have been collected whilst you were living at an address other than your current one, it may be useful to supply us with that address in order that we can access the information more quickly.

Locating your records : SATCoL is a large organisation with many different Divisions dealing with a diverse range of services. Completing this section will ensure that your request is delivered to the correct area of SATCoL and therefore dealt with more quickly and efficiently.

SATCoL will not release information without proper authority, and reserves the right to request further proof of authority or identity if necessary.