|  |  |
| --- | --- |
| **Document Reference** | GDPR-01 GDPR Data Protection Policy – V1.7 |
| **Date** | 28th January 2020 |
| **Document Status** | Final Release version |
| **Version** | 1.6 |
| **Revision History** | 1.0: 4th April 2018 – Draft produced  1.1: 14th April 2018 – Draft continued  1.2: 24th April 2018 – Reviewed with ISM / IT  1.3: 30th April 2018 – Reviewed by GDPR committee  1.4: 6th May 2018 – Final Draft continued  1.5: 11th May 2018 – Final version and release  1.6: 12th August 2019 – Updated Draft version  1.7: 28th January 2020 – Final version and release |
| **Owner** | Data Protection Officer |
| **Classification** | Public |
| **Distribution** | All Locations / Levels |

**Table of Contents**

1. Introduction ………………………………………………………………….………….3

2. Objectives….……………………………………………………………….……………. 3

3. Data Protection Law………………………………………………….……………….3

4 People Risks and Responsibilities………………………………..……………..4

* Policy Scope…………………………………………………………………..….….4
* Data Protection Risk…………………………..………………………….….….4
* Data Protection Framework………………………………………………....4

5. Governance……………………..………………………………………………………...5

6. Responsibilities…………………………………………………………..……………… 5

* The Board of Directors….……………………………………………………… 5
* The Data Protection officer…….…………………………………….….……5
* IT…………………………………….………………………………………..….…..……6
* Marketing…………………….………………………………………………….….…6

7. General Colleague Guidelines……………………………………………..…..….6

8. Data Storage…..………………………………………………………………..…….…..6

9. Data Use…………..…………………………………………………………………….…..7

10. Data Accuracy……………..………………………………………………………….…..7

11. Subject Access Requests…………………………..…………………………….……7

12. Disclosing Data for other reasons…..…………………………………….……..8

13. Fair Processing……………………………………………………………………..………8

14. Revisions …………………………………………………………………………….….…...8

15. Related Documents ……………………………………………………………...……..9

**Appendix A** - Information Notification to Data Subjects

**Appendix B** - Adequacy for Personal Data Transfers

**Appendix C** - Data Protection for Colleague Data policy

**Appendix D** - Web Site Customer Privacy Notice

**Appendix E** - Hobbycraft Data Retention Guidelines

**Appendix F** - P01- Information Security Policy

**Appendix G** - Data Subject Request Handling Procedures

**Appendix H** - Subject Access Request Form

**Appendix I** - Standard Data Processing Agreement

**(Above Appendix documents on VPA - Knowledge base)**

**GDPR Data Protection Policy**

**Introduction**

Hobbycraft Trading Ltd needs to collect and use certain information about individuals to manage the people who are working with it and to provide services to people looking to buy from our online store.

This can include customers, suppliers, colleagues, consultants, contractors and other people with whom the organisation has a relationship.

This policy describes how this personal data must be collected, handled and stored to meet Hobbycraft’s data protection standards and demonstrate compliance with data protection legislation.

**Objectives**

This data protection policy ensures Hobbycraft:

* Complies with data protection law and follows good practice.
* Protects the rights of colleagues, customers and partners.
* Is fair and transparent in how it collects, processes and shares personal data.
* Reduces the likelihood of a data breach.

**Data Protection law**

The General Data Protection Regulation 2018 (GDPR) and the Data Protection act 2018 sets out how organisations, including Hobbycraft, must collect, process and share personal data.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

Under the GDPR and Data protection act, the data protection principles set out the main responsibilities for organisations. Hobbycraft must be responsible for and be able to demonstrate that personal data is:

1. Processed fairly and lawfully
2. Obtained only or specific lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not be held for any longer than necessary
6. Secure and protected.

**People, Risks and Responsibilities**

**Policy Scope**

This policy applies to:

* Hobbycraft Head office.
* All retail stores, Distribution centre and offices of Hobbycraft.
* All colleagues regardless of work level.
* All contractors, suppliers and other people working on behalf of Hobbycraft.

It applies to all personal data that the company holds. This includes:

* Customer information e.g. on line Hobbycraft club accounts and online purchases information.
* Colleagues details e.g. Health information, financial details, benefits and pensions.

**Data Protection Risks**

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

* Breaches of confidentiality. For example, information being given out inappropriately, sharing too much information, or sharing without consent or other lawful basis.
* Failing to offer choice and transparency. For instance, not informing individuals how their information will be used and how they can exercise their rights.
* Reputational damage. For instance, the company could suffer if hackers successfully gained access to our sensitive data.

**Data protection framework**

Hobbycraft has put in place a Data Protection Framework, which includes policies, procedures, guidance and records. This includes:

* + Business compliance processes and procedures such as colleague awareness training to ensure that we think about data protection and its implications before going down a particular route. Related policies which provide further detail include:
    - Information Security
    - Subject Access Request
    - Incident management
    - Supplier Management
    - Access Control
    - Clear Desk
    - Classification and handling
    - Retention
* Where to go for help
  + Email: [dataprotection@hobbycraft.co.uk](mailto:dataprotection@hobbycraft.co.uk)
  + Line Manager
  + Data Protection Officer: [privacy@hobbycraft.co.uk](mailto:privacy@hobbycraft.co.uk)
* Privacy and Security by Design embedded into projects and operational processes
  + Documented records of processing in our Information Asset Inventory
  + Data Protection Impact Assessments
  + Change Control.

**Governance**

All staff should be aware of the structures in place for suppler assurance, risk identification, breach reporting, and subject access requests. Functional steering groups are in place to ensure the consistent application of the framework and that its operation is fit for purpose, efficient and effective.

**Responsibilities**

Everyone who works for or with Hobbycraft has some responsibility for ensuring data is collected, stored, processed and shared appropriately.

Each team that handles personal data must ensure that it is processed in line with this policy and the data protection principles.

In addition to this, a number of people have specific areas of responsibility:

* **The board of directors** are ultimately responsible for ensuring that Hobbycraft meets its legal obligations.
* **The Data Protection Officer -** [**privacy@hobbycraft.co.uk**](mailto:privacy@hobbycraft.co.uk) **is responsible for:** 
  + Keeping the board updated about data protection responsibilities, risks and issues
  + Reviewing all data protection procedures and related policies in line with an agreed schedule to ensure they remain up to date and effective
  + Arranging data protection training and advice for the people covered by this policy
  + Dealing with requests from individuals to see the data Hobbycraft hold about them (Subject Access Requests)
  + Handling data protection questions from colleagues and anyone else covered by this policy
  + Checking and approving any contracts or agreements with 3rd parties that may handle personal data
  + Review and sign-off of data protection impact assessments.

* **IT {email] is responsible for:** 
  + Ensuring all systems, services and equipment used for storing personal data meet acceptable security standards
  + Performing regular checks and scans to ensure security hardware and software is secure and fit for purposes
  + Evaluating any 3rd party services the company is considering using to store of process personal data.
* **Marketing {email} is responsible for:** 
  + Approving any data protection statements attached to communications such as emails and letters and online.
  + Where necessary, working with other staff to ensure marketing initiatives abide by the data protection principles.
  + To ensure marketing databases are checked against industry suppression files every six months.

**General colleague guidelines**

To ensure the objectives of this policy are met, Hobbycraft has outlined guidance below to reduce the likelihood of the most common reasons for breaches of information.

* The only people able to access data covered by this policy should be those who **need it to for their work.**
* Data should **not be shared informally**.
* **Hobbycraft will provide training** to all colleagues to help their responsibilities when handling data.
* **Strong passwords must be used** and they should never be shared unless authorised by IT.
* **Personal data should not be disclosed** to unauthorised people, either within the company or externally.
* Colleagues **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

**Data storage**

These rules describe how and where data should be safely stored.

**Paper records:**

* When not required, paper files should be **kept in a locked drawer or filling cabinet.**
* Colleagues should make sure paper and printouts are **not left where unauthorised people could see them** (e.g. on a printer).
* Data Printouts should be **shredded and disposed of securely** when no longer required.

**Electronic records:**

* Data should be **protected by strong** passwords that are never shared.
* If data is stored on removable media (e.g. USB, DVD) these should be kept **locked away when not being used.**
* Data should only be stored on **designated drives and servers** and should only be uploaded to **approved cloud computing services**.
* Servers containing personal data should **be sited in a secure location**, away from general office space.
* Data should be **backed up frequently**. These backups should be tested in line with company standard backup procedures.
* Data should **never be saved directly** to laptops or other mobile devices.

**Data use**

* When working with personal data, colleagues should ensure the **screens of their computers are always** locked when unattended.
* Personal data **should not be shared informally**. In particular it should never be sent by email, as this form of communication is not secure.
* Data must **be encrypted before being transferred electronically**. IT department can advise on how to send data to authorised external contacts.
* Personal data should **never be transferred outside the European Union** without consulting the Data Protection officer.
* Colleagues should **not save copies of personal data to their own computers.**

**Data Accuracy**

It is important that the data we process is accurate and, where necessary, kept up to date. The more important the information the greater the effort Hobbycraft should put into ensuring its accuracy.

* Data should be **held in as few places as necessary**. Colleagues should not create any unnecessary additional data sets.
* Colleagues **should take every opportunity to ensure data is updated**. For instance by confirming a customer details when they call.
* Hobbycraft will make it **easy for data subjects to update the information Hobbycraft holds about them** (e.g. via online web portal).
* Data should be **updated as soon as inaccuracies are discovered**.

**Subject access requests**

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

* Request what information Hobbycraft holds about them and why.
* Ask for a copy the information we hold about them.
* Be informed how to keep it up to date.
* Be informed how to object to processing.
* Be informed about how their data is being used.
* Be informed about the security safeguards in place to prevent accidental or deliberate disclosure of their information.

If an individual contacts the company requesting this information, it is called a subject access request (SAR).

Subject access requests are addressed in a separate procedure, “Data Subject Request Handling Procedure”.

**Disclosing data for other reasons**

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

Under these circumstances, Hobbycraft will disclose the requested data. However, the Data Protection officer must be informed prior to any such disclosure to ensure the request is legitimate and follows due process.

**Fair Processing**

Hobbycraft aims to ensure that individuals are aware that their data is being process and that they understand:

* How their data is being used.
* How to exercise their rights.

To these ends, Hobbycraft has a Privacy Policy, setting out how data relating to individuals is used by the company. This is available on Hobbycraft’s website.

**Revisions**

The Data Protection officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the IMS.

A current version of this document is available to all colleagues on the company network and is published.

**Related Documents**

There are other documents that are either referenced here or are relevant to the operation of this policy. These are made reference to as APPENDIX Documents. (All available on Knowledge Base)

Listed below are documents that relate to this policy;

* Web Site Customer Privacy Notice
* P01 - Information Security Policy
* Data Subject Request Handling Procedure
* Data Subject Access Request Form
* Data Protection for Colleague Data Policy
* Hobbycraft Data Retention Guidelines
* Standard Data Processing Agreement

This policy was reviewed by the Data Protection Officer and is issued on a version controlled basis under his signature;

Signature: Date: