Table of Contents

Overview 3

Introduction 4

Why this Policy Exists 4

Data Protection Law 4

People, Risks and Responsibilities 6

Policy Scope 6

People 6

Responsibilities 7

General Data Protection Policy Information 8

Data Storage 9

Data Access and Accuracy 10

Disclosure 11

Data Protection Training 12

Non-Conformance 13

Policy Prepared by:
John Church

Approved by:
John Church

24.5.18
Policy became operational on: 24.5.18
Next Review date: 1st January 2019

Data Controller
John Church is the Data Controller under the General Data Protection Regulation, which means that it determines what purposes personal information held, or will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

John Church is registered with the Information Commissioner's Office as a Data Controller.

BRIEFED™

Overview

There is a suite of documents, which together make up the Data Protection policies of John Church .

This General Data Protection Policy should be read in conjunction with the following documents.

1. Mobile Working Policy
2. Data Retention and Disposal Policy
3. Subject Access Request Policy
4. Data Breach Checklist
5. Data Sharing Agreement where appropriate.
6. Data Processed Register
7. Data Protection Training Register
8. Near Miss Register
9. Third Party Data Sharing Register
10. IT Register

Introduction

John Church needs to gather and use certain information about individuals.

These can include clients, customers, suppliers, business contacts, employees and other people the practice has a relationship with or may need to contact.

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

Why this Policy Exists

This data protection policy exists to ensure that John Church;

- Complies with Data Protection law and follows good practice
- Protects the rights of staff, clients, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach.

Data Protection Law

The General Data Protection Regulation describes how organisations must collect, 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 General Data Protection Regulation is underpinned by six important principles. They say that personal data must be:

1. processed lawfully, fairly, and transparently
2. collected for specific, explicit, and legitimate purposes
3. adequate, relevant, and limited to what is necessary for processing
4. accurate and, where necessary, kept up to date.

5. kept in a form such that the Data Subject can be identified only as long as is necessary for processing and professional obligations
6. processed in a manner that ensures appropriate security of the personal data

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation.

BRIEFED™

People, Risks and Responsibilities

Policy Scope

People

This policy applies to:
All employees of John Church - that includes management, clerks, trainees, volunteers, work experience students, support staff.
All contractors, suppliers and other people working on behalf of John Church

It applies to all data the practice holds relating to identifiable individuals. This can include but is not limited to:

> Names of individuals, postal addresses, email addresses, telephone numbers, financial data, business names, plus any other personal sensitive information relating to individuals.

BRIEFED™

Responsibilities

Everyone who works for John Church has responsibility for ensuring data is collected, stored and handled appropriately.

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation.

BRIEFED™

General Data Protection Policy Information

John Church will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational / professional needs or to comply with any legal / professional requirements / obligations
- Ensure the quality of information used
- Ensure appropriate retention and disposal of information consistent with professional obligations
- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erase
  - The right to restrict processing so far as this is consistent with professional obligations
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling.

- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred outside the EEA without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information subject to appropriate professional confidentiality

BRIEFED™

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and data processors.

Information will be stored for only as long as it is needed or required statute / professional obligations and will be disposed of appropriately.

John Church will ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

BRIEFED™

Data Access and Accuracy

All individuals/data subjects have the right to access the information John Church BARRISTER holds about them, except where specific exemptions apply to a legal professional. John Church BARRISTER will also take reasonable steps ensure that this information is kept up to date in relation to professional obligations .

In addition, John Church will ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody interested in making enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

BRIEFED™

Disclosure

John Church may share data with other agencies such as government departments and other relevant parties as is necessary in the performance of his professional obligations .

The Individual/data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows John Church to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of an individual/data subject or other person

c) The individual/data subject has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the individual/data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill individuals'/data subjects to provide consent signatures.

BRIEFED™

Data Protection Training

John Church will ensure that he and all employees are appropriately trained in Data Protection and particularly the policies of John Church and the barristers at Fieldcourt Chambers annually.

If new members of staff commence work with John Church, or at Fieldcourt Chambers they will be provided with data protection training within the first month of employment.

John Church, or Fieldcourt Chambers keeps a register of all training provided to staff.

BRIEFED™

Non-Conformance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

In case of any queries or questions in relation to this policy please contact the John Church Data Protection Officer:

Name and contact details of the Data Protection officer:

NAME John Church
John.church@fieldcourt.co.uk