Name of policy	Data Protection Policy
Brief description	This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the CEO should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.
Date of review	Oct - 2019
Version Control	Next Review Aug - 2020, Version 1.0

Introduction

Justice and Care does all it can to protect the privacy and protect the personal data of everyone who engages with us, by whatever means.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation which strengthens and unifies data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR replaces the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applied from 25 May 2018 after a two-year transition period..

The Regulations cover both written and computerised information and the individual's right to see such records. It is important to note that the Regulations also cover records relating to staff and volunteers.

Scope

This policy applies to all staff and volunteers. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to Use of the Employer's Electronic and Computer Facilities. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

The CEO has overall responsibility for this policy. They are responsible for ensuring this policy is adhered to by all staff.

The Chief Executive has overall responsibility for data protection within Justice and Care but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations. In particular, this policy requires staff to ensure that the CEO should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Processing of information – how information is held and managed.

Information Commissioner - formerly known as the Data Protection Commissioner.

Notification – formerly known as Registration.

Data Subject – used to denote an individual about whom data is held.

Data Controller – used to denote the entity with overall responsibility for data collection and management. Justice and Care is the Data Controller for the purposes of the Act.

Data Processor – an individual handling or processing data

Personal data – any information which enables a person to be identified

Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Charity.

Data Protection Principles

As data controller, Justice and Care is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data **fairly**, **lawfully and in a transparent manner.**
2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate**, **relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).

- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

- Individuals have a right to have their data erased and to prevent processing in specific circumstances:

- Where data is no longer necessary in relation to the purpose for which it was originally collected
- When an individual withdraws consent
- When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- Personal data was unlawfully processed

· An individual has a right to restrict processing – where processing is restricted, Justice and Care is permitted to store the personal data but not further process it. Justice and Care can retain just enough information about the individual to ensure that the restriction is respected in the future.

· An individual has a 'right to be forgotten'.

Data Subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Justice and Care) must comply with such requests within 30 days of receipt of the written request.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless:

- the individual whose details we are processing has consented to this
- the processing is:
  - necessary to perform legal obligations or exercise legal rights, or
  - otherwise in our legitimate interests and does not unduly prejudice the individual's privacy

In most cases this provision will apply to routine business data processing activities.

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's EXPLICIT consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. We use a consent form for these purposes. Please see form reproduced below.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the CEO.

Staff and volunteer personal data

The Regulations apply equally to volunteer and staff records. Justice and Care may at times record special categories of personal data with the volunteer's consent or as part of a staff member's contract of employment.

For staff and volunteers who are regularly involved with children or vulnerable adults, it will be necessary for Justice and Care to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Senior Management Team. If there is a positive disclosure the Chief Executive will discuss this, anonymously, with the Chair and our insurers to assess the risk of appointment. Trustees and insurers should not see the report itself.

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required, eg if your personal circumstances change then please inform your line manager/the HR lead so that they can update your records.

Data security

You must keep all personal data secure against loss or misuse and comply at all times with the data security policy and procedure. Where other organisations process personal data as a service on our behalf, the CEO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our Data retention guidelines below.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data internationally at all without first consulting the CEO.

Subject access requests

Please note that under the Data Protection Act 2018, individuals are entitled (subject to certain exceptions) to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the CEO. We may ask you to help us comply with those requests.

Please contact your Team Leader / line manager if you would like to correct or request information that we hold about you. We may charge a small fee for providing personal data about you if the request is excessive or manifestly unfounded. There are also restrictions on the information to which you are entitled under applicable law.

REPORTING BREACHES

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures
- notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Manager for full details of our reporting procedure. The CEO should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the Board of Trustees. There is a time limit for reporting breaches to ICO so the CEO should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

TRAINING

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures
- Completion of training is compulsory.

The CEO will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our data protection policy or procedures, please contact your team leader or line manager.

MONITORING

Everyone must observe this policy. The CEO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

CONSEQUENCES OF FAILING TO COMPLY

- We take compliance with this policy very seriously.
- Failure to comply puts both you and the organisation at risk.
- The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.
- If you have any questions or concerns about anything in this policy, do not hesitate to contact your Team Leader or line manager.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.

- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further information is available at www.informationcommissioner.gov.uk

Detailed operational guidelines:

Consent for service users

Justice and Care must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

1. The racial or ethnic origin of the Data Subject.
2. His/her political opinions.
3. His/her religious beliefs or other beliefs of a similar nature.
4. Whether he/she is a member of a trade union.
5. His/her physical or mental health or condition.
6. His/her sexual life.
7. The commission or alleged commission by him/her of any offence
8. Online identifiers such as an IP address
9. Name and contact details
10. Genetic and/or biometric data which can be used to identify an individual

Special categories of personal information collected by Justice and Care regarding service users may include any of the above.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule Justice and Care will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the relevant Manager or Chief Executive for advice.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email

Face-to-face/written

A pro-forma should be used.

Telephone
Verbal consent should be sought and noted on the case file

E-mail
The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the

provision of that service, separate consent would be required if, for example, direct marketing were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record (e.g. Charitylog). The verbal consent is to be recorded in the appropriate fields on the CMS. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in accordance with the photo video and story permissions policy. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by Justice and Care then this should be discussed with the relevant Manager at the earliest opportunity.

Ensuring the Security of Personal Information

All staff and volunteers must follow the data security protocol at all times. Failure to do so may result in disciplinary action.

Unlawful disclosure of personal information

1. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

2. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.

3. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.

4. A client's individual consent to share information should always be checked before disclosing personal information to another agency.

5. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive or relevant Manager should first be sought.

6. Personal information should only be communicated within Justice and Care's staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

7. The detailed data security policy and procedure must be followed by all staff and volunteers at all times

Consent for direct marketing and newsletters

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc.). The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. Justice and Care will not share or sell its database(s) with outside organisations.

Justice and Care holds information on our staff, volunteers, clients and other supporters, to whom we will from time to time send copies of our email updates, annual report and details of other activities that may be of interest to them. Specific consent to contact will be sought from our staff, clients and other supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications.

We recognise that clients, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

As standard for all documents gathering personal information the following wording should be used:

Justice and Care is a charity committed to fighting slavery and human trafficking. We will only store and use your personal data for the purpose it was given and with your consent. We will keep your data secure and will never share it with third parties. We store your data only for as long as necessary for the purpose you gave it, and you can have your data removed or opt out of communications at any time by contacting us - see www.justiceandcare.org/privacy-policy

The full privacy policy detailed on the website is a separate document to be read in conjunction with this policy - available at **https://www.justiceandcare.com/privacy-policy/**

SENSITIVE DATA PROCESSING CONSENT FORM

The information we gather:
Justice and Care gathers certain information about you.
We may gather information directly from you or from third parties, such as government agencies, the police and law enforcement organisations, service providers, referrers, partner agencies, and former employers.

Transferring Data Internationally
Information may be transferred internationally to the Netherlands, the US, and to other countries around the world where Justice and Care have their operations, including those without data protection laws equivalent to those in the UK, for the reasons described below.

Sensitive personal data
You may also supply us with sensitive personal data relating to your racial or ethnic origin/ political opinions/religious or similar beliefs/trade union membership/physical or mental health/criminal record which is gathered for the reasons listed below.

Reasons for processing and gathering information
We process information about you for the following reasons:
1. compliance with legal, regulatory and corporate governance obligations and good practice
2. ensuring business policies are adhered to
3. checking personal and employment background to ensure suitability for employment
4. operational reasons, such as data management, training and quality control
5. ensuring safe working practices, monitoring and managing staff access to systems
6. staff administration and assessments, monitoring staff conduct, disciplinary matters

Disclosures and exchange of information
We may exchange information with other professionals /law enforcement agencies/ regulatory bodies/other for the above reasons.

Further enquiries
Please contact the Compliance Manager if you would like to correct or request information that we hold relating to you or if you have any questions in relation to the above. We may charge a small fee for providing personal data about you as permitted by law, under exceptional circumstances. This will be no more than £10.

Consent
I consent to the processing of information (including sensitive personal data) as described above.

Name:

Date:

[SIGNATURE: IF PAPER CONSENT]

[TICK BOX: IF ELECTRONIC CONSENT]

Data retention guidelines

Please note that these are guidelines only, which set MINIMUM retention periods for both physical files and electronically held data. If there is a genuine business need to retain data for a longer period, please contact the CEO.

Anti-money laundering records

1. Records of client identity and verification checks made under our client due diligence procedure must be retained for FIVE YEARS after the business relationship ends or the transaction completes.
2. **Client files**

Matter type	Retention period
Investigations	Indefinite
Tax	**12 years** after the end of the trust period or assessment
Financial services (transactions and commissions effected or received under the SRA Financial Services (Conduct of Business) Rules 2001)	**6 years**
All other client matter files	**6 years**

3. **Central business records**
    a. **ACCOUNTS RECORDS** **6 years**.
    b. COMPLAINTS RECORDS - 6 years from the conclusion of the complaint
4. **HR records**

Record type	Retention period
Accident books, reports and records	**3 years** from the date of the last entry (if an accident relates to a child or young adult—until that person reaches 21 years)
Income tax and NI records and correspondence with HMRC	**3 years** after the end of the financial year to which they relate
Retirement Benefits Schemes—notifiable events	**6 years** from the end of the scheme year in which the event took place
Statutory Maternity Pay records	**3 years** after the end of the tax year in which the maternity period ends

Statutory Sick Pay records	**3 years** after the end of the tax year to which they relate
Salary and pay records	**6 years**
Application forms and interview notes for unsuccessful candidates (the same data for successful candidates will be transferred to their Personnel files—see **Personnel files** below)	[**6 MONTHS/1 YEAR**]
Parental leave records	**5 years** from the birth or adoption of the child or **18 years** if the child receives a disability allowance
Pension scheme investment policies	**12 years** from the end of any benefit payable under the policy
Personnel files and training records (including disciplinary records and working time records)	**6 years** after employment ceases
Redundancy records	**6 years** from date of redundancy
Other HR records	[**1 YEAR/2 YEARS**]

5. **Fundraising records -** **6 years** from the end of the accounting period they relate to, in line with HMRC guidelines on Gift Aid donations.