BRISTOL CHARITIES
DATA PROTECTION POLICY

January 2020

.

BRISTOL CHARITIES

CONTENTS

1 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify 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. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period.

1.2 The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations but seeks to interpret relevant points where they affect Bristol Charities.

1.3 The Regulations cover both written and computerised information and the individual's right to see such records.

1.4 It is important to note that the Regulations also cover records relating to staff and volunteers.

1.5 All Bristol Charities staff are required to follow this Data Protection Policy at all times.

1.6 The Chief Executive has overall responsibility for data protection within Bristol Charities, but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

2 DEFINITIONS

2.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

2.2 **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. Bristol Charities 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.

3 DATA PROTECTION PRINCIPLES

3.1 As Data Controller, Bristol Charities is required to comply with the principles of good information handling.

3.2 These principles require the Data Controller to:

(a) Process personal data fairly, lawfully and in a transparent manner

(b) 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

(c) Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held

(d) Ensure that personal data is accurate and, where necessary, kept up to date

(e) Ensure that personal data is not kept for any longer than is necessary for the purpose it was obtained

(f) Ensure that personal data is kept secure

(g) 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

4 CONSENT

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

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

(a) The racial or ethnic origin of the Data Subject

(b) His/her political opinions

(c) His/her religious beliefs or other beliefs of a similar nature

(d) Whether he/she is a member of a trade union

(e) His/her physical or mental health or condition

(f) His/her sexual life

(g) The commission or alleged commission by him/her of any offence

(h) Online identifiers such as an IP address or email address

(i) Name and contact details

(j) Genetic and/or biometric data which can be used to identify an individual

4.3 Special categories of personal information collected by Bristol Charities will, in the main, relate to service users' physical and mental health and financial status. Data is also collected on ethnicity and sexuality and held confidentially for statistical purposes.

4.4 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.

4.5 As a general rule Bristol Charities will seek consent where personal or special categories of personal information is to be held.

4.6 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.

4.7 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 Services Manager or Chief Executive for advice.

5 OBTAINING CONSENT

5.1 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

5.2 **Face to face written** – a pro-forma should be used

5.3 **Telephone** – verbal consent should be sought and noted on the case record

5.4 **Email**- the initial response should seek consent

5.5 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 was to be undertaken.

5.6 Preliminary verbal consent should be sought at the 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 (charitylog). The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

5.7 Specific consent for use of any photographs and/or videos taken should be obtained in writing. 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 must be sought.

5.8 Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by Bristol Charities, then the member of staff should discuss with the Service Manager at the earliest opportunity.

6 ENSURING THE SECURITY OF PERSONAL INFORMATION

6.1 Unlawful disclosure of information:

1. It is an offense 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 to prevent substantial risk to the individual-

concerned. In either case, permission of the Chief Executive or Service Manager should be first sought.

6. Personal information should only be communicated within Bristol Charities 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 overhead by people who should not have access to such information.

7. Security questions should be asked to check the identity of anyone requesting personal information by phone.

7 ETHNIC MONITORING

7.1 For Bristol Charities to monitor how well our staff, volunteers and service users reflect the diversity of the local community we request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a pass-worded database for statistical purposes.

8 USE OF FILES, BOOKS AND PAPER RECORDS

8.1 To prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working day. If your work involves you having personal and/or special categories of personal data at home or in your care, the same care needs to be taken.

9 DISPOSAL OF SCRAP PAPER, PRINTING OR PHOTOCOPYING OVERRUNS

9.1 Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

9.2 If you are transferring papers from your home, or your clients home, to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents, they should be carried out of sight in the boot of your car.

10 COMPUTERS

10.1 Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

10.2 Computer monitors in the reception/office areas or other public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, e.g. reception, you should lock your computer when leaving it unattended.

10.3 Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

10.4 Documents should only be stored on the server or cloud-based systems and not on individual computers.

10.5 Where computers or other mobile devices are taken for use off the premises the device must be password protected.

11 CLOUD COMPUTING

11.1 When commissioning cloud-based systems, Bristol Charities will satisfy themselves as to the compliance of data protection principles and robustness of the cloud-based providers.

11.2 Bristol Charities currently uses cloud-based data management systems to hold and manage information about its service used:

Office 365 is accredited to ISO 27001, Information Security Standard, European Union (EU) Model Clauses, the Health Insurance Portability and Accountability Act Business Associate Agreement (HIPAA BAA), and the Federal Information Security Management Act (FISMA). Office 365 has built over 900 controls into its compliance framework that enables industry standards to be kept up to date. A dedicated team continuously tracks standards and regulations. As such Bristol Charities is satisfied with the security levels in place to protect its data.

12 DIRECT MARKETING

12.1 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. Bristol Charities will not share or sell its database(s) with outside organisations.

12.2 Bristol Charities holds information on our staff, volunteers, clients and other supporters, to whom we will from time to time send copies of our newsletters, magazine 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 (e.g. mail, email, phone etc.) before making any communications.

12.3 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.

12.4 The following statement is to be included on any forms used to obtain personal data: We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning: 01179 300301, by writing to: Bristol Charities, 17 St Augustine's Parade, Bristol, BS1 4UL, or by emailing: info@bristolcharities.org.uk

13 PRIVACY STATEMENTS

13.1 Any document 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

13.2 A fuller Privacy Statement will also be published on our website.

14 PERSONNEL RECORDS

14.1 The Regulations apply equally to volunteer and staff records. Bristol Charities 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.

14.2 For staff and volunteers who are regularly involved with vulnerable adults, it will be necessary for Bristol Charities 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 of the Audit Committee and our insurers to assess the risk of appointment. Trustees and insurers will not see the report itself.

15. CONFIDENTIALITY

15.1 Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

15.2 When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for Bristol Charities should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer they should be saved onto a USB drive which will be password protected.

15.3 Workstations in areas accessible to the public, e.g. reception office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

15.4 When sending emails to outside organisations, e.g. social worker or hospital staff, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be watermarked confidential.

15.5 Any paperwork kept away from the office (e.g. support plans kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g. on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Staff needing to take paperwork away from a client's home (e.g. unable to make a required phone call during the visit) must ensure that it is returned to the client's home on the next visit.

15.6 If you are carrying documents relating to several clients when on a series of home visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them to into the client's home. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain Bristol Charities contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

16. RETENTION OF RECORDS

16.1 Paper records should be retained for the following periods at the end of which they should be shredded.

- Grant Applications – 2 years
- Client records – 6 years after ceasing to be a client
- Staff records – 6 years after ceasing to be a member of staff
- Unsuccessful staff application forms – 6 months after vacancy closing date
- Volunteer records – 6 years after ceasing to be a volunteer
- Timesheets and other financial documents – 7 years
- Employer's liability insurance – 40 years
- Other documentation, e.g. clients care plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand

16.2 Archived records should clearly display the destruction date.

16.3 Computerised records e.g. demographic area/reason grant awarded is to be anonymised 6 years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.

17. WHAT TO DO IF THERE IS A BREACH

17.1 If you discover, or suspect, a data protection breach, you should report this to your line manager who will review our systems, in conjunction with the Senior Management Team, to prevent a reoccurrence. The Chief Executive Officer 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 Information Commissioner, so the Chief Executive Officer should be informed without delay.

17.3 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.

18. THE RIGHTS OF AN INDIVIDUAL

18.1 Under the Regulations an individual has the following rights regarding the processing of his/her data:

18.2 The right to be informed. This includes how the information you supply about the processing of personal data must be – typically in a privacy notice.

18.3 The right of access to an individual's data free of charge. Response must be within one calendar month.

18.4 The right to rectification. Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. Response to a rectification request should be one calendar month.

18.5 The right to erasure or the right to be forgotten. Personal data must be removed or deleted securely when there is no compelling reason for possession and continued processing. Data cannot be used for the purpose of direct marketing of any goods or services if the data subject has declined their consent to do so, or not given their consent initially.

18.6 The right to restrict processing. Individuals have the right to block or restrict processing of personal data, in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing should be restricted until the accuracy of personal data has been verified
- Where an individual has objected to the processing and it is being considered whether the charity's legitimate grounds override those of the individual
- When processing is unlawful and the individual opposes erasure and requests restriction instead
- If the personal data is no longer needed by the charity but the individual requires the data to establish, exercise or defend a legal claim

18.7 The right to data portability. This allows individuals to obtain and revise their personal data across different services for their own purposes

18.8 The right to object. This means that individuals have the right to object to direct marketing and processing based on legitimate interest and purposes of scientific historical research and statistics

19. POWERS OF THE INFORMATION COMMISSIONER

19.1 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

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

19.3 The Information Commissioner's Office is at:
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Switchboard: 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

20. IMPLEMENTATION AND MONITORING

20.1 Implementation is immediate, and this Policy shall stay in force until any alterations are formally agreed.

20.2 The Policy will be reviewed every two years by the Board of Trustees, sooner if legislation, best practice or other circumstance indicate this is necessary.

20.3 All aspects of this policy shall be open to monitoring and review at any time. If you have any comments or suggestions the content of this policy, please contact Bristol Charities at info@bristolcharities.org.uk

21. OTHER RELATED POLICIES AND PROCEDURES

- Privacy Statement
- Confidentiality Policy
- Disciplinary Policy
- Safeguarding Vulnerable Adults
- Retention, Archiving and Destruction of Information Guidance