BRISTOL CITY COUNCIL

DATA PROTECTION POLICY

15th May 2018

CONTENTS:

1. POLICY STATEMENT

1.1

Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our citizens, service users, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful service delivery.

1.2

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1

The types of personal data that Bristol City Council (BCC) may be required to handle include information about current, past and prospective customers, service users, employees, suppliers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations EU 2016/679 (the Regulation), the Data Protection Act 2018 (the Act) and other regulations related to personal data.

2.2

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3

This policy is non-contractual and may be amended at any time.

2.4

This policy has been approved by the Information Assurance Group of the Council. It leads and advises on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5

The Data Protection Officer is responsible for ensuring Bristol City Council's compliance with data protection legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer, Bristol City Council, City Hall, PO Box 3176, Data.protection@bristol.gov.uk

3. DEFINITION OF DATA PROTECTION TERMS

3.1

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

3.2

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3

Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. Examples of online identifiers include IP addresses, online screen names and browser cookies.

3.4

Data controllers are the people or organisations that determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection legislation. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5

Data users are those of our employees whose work involves processing personal data. They work on behalf of Bristol City Council (who is the Data Controller). Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times- including abiding by the Employee Code of Conduct.

3.6

Data processors include any person or organisation that is not employed by BCC that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition for the purposes of BCC-mandated tasks but it could include suppliers which handle personal data on BCCs and third parties that may provide technical support.

3.7

Processing is any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

3.8

Special category data (formerly known as **Sensitive Personal Data**) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or any genetic or biometric data. Special category data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3.9

Criminal offence data includes information about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. This data requires a legal basis for processing (as with all personal data) but can only be processed in an official capacity or where the council has specific legal authorisation under other legislation.

4. DATA PROTECTION PRINCIPLES

4.1

Anyone processing personal data must comply with the six enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly, lawfully and transparently.

(b) Collected for explicit, legitimate purposes and not processed further than stated to the subject.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) Accurate and up to date.

(e) Not kept in an identifiable form for longer than necessary for the purpose.

(f) Secure and monitored.

5. FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1

Data protection law is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, necessary to protect the vital interests of the data subject or necessary to carry out tasks that are in the public interest. When special category data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met. A contract must be in place with all data processors and that this will be compliant with data protection legislation.

5.3

A record of all processing activity will be maintained by those responsible for holding data. This will include personal data that we are chiefly responsible for as well as all data processed for a third party, and document all transfers, security processes, legal bases for processing and locations of storage.

5.4

We will maintain a standard of privacy by design, by which all new projects, services and changes will be built with privacy and data protection as a key consideration. This includes undertaking a privacy impact assessment (PIA) for all processing that is considered to be high risk.

5.5

We shall provide a privacy notice to all data subjects at the point at which we collect their data, informing them of our intentions to process their data and how we intend to do it. This must be specific for the processing operation.

6. PROCESSING FOR LIMITED PURPOSES

6.1

In order for us to deliver our services, we collect and process personal data for specific purposes which we will inform our data subjects about. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, partner organisations, local authorities, central government, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2

We will only process personal data for specific purposes or for any other purposes specifically permitted by the

Regulation or the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1

If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The third parties or types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

(d) The legal basis we have for processing data

(e) The identity and contact details of the data controller, the data protection officer and any other parties relevant to the processing of their data

(f) The length of time we intend to retain the data for (or, if not known, the methodology used to determine the retention period)

(g) The use of automated decision making or profiling (automated processing of personal data to evaluate certain things about an individual) where applicable

7.2

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible, within one month of receiving the data, upon first contact with the data subject, or when the data is transferred to another recipient.

7.3

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and the contact details of the Data Protection Officer.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8.1

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject and within their reasonable expectations.

9. ACCURATE DATA

9.1

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

10.1

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

11.1

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also *Clause 15.*).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also *Clause 9.*).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

(e) Move, copy or transfer easily from one database to another safely and securely without hindrance to usability.

(f) Be informed on the nature of the processing taking place, through the use of tailored privacy notices specific to each service provided to them.

12. DATA SECURITY

12.1

We will process all personal data we hold in accordance with our Information Security Policy.

12.2

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself. Sub-processors will not be appointed without the approval of the data controller.

12.3

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on BCCs central computer system instead of individual PCs.

12.4

Security procedures include but are not limited to:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported. All BCC Staff should have their staff ID card on them at all times when within BCC property.

(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required, or sanitised in accordance with the BCC Secure Sanitisation Standard. Disposal of data should be recorded.

(d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended, or otherwise apply the screen lockout function. Only portable media devices that have been encrypted may be used.

(e) Information Security Guide: All staff must have read and apply the provisions of the Information Security Guide.

(f) Training: All staff including casual staff and contractors must complete Information Security and Data Protection training before being allowed access to BCC network. Such training must be confirmed on staff appraisals (My Performance) and, must be refreshed, at minimum, annually otherwise access to the BCC network will be revoked. It is the responsibility of line managers to ensure such training is completed.

13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

13.1

We may only transfer any personal data we hold to a country outside the European Economic Area (”EEA”), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects’ rights and freedoms.

(b) The data subject has given consent.

(c) The transfer is necessary for one of the reasons set out in the Regulation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or

defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1

We may share personal data we hold across council services in accordance with the privacy statement provided to data subjects, either at the point of initial contact or via our website.

14.2

We may also disclose personal data we hold to third parties:

(a) This may include contractors (processors) who work for us to deliver our services; A contract will be in place with all data processors and that this will be compliant with the Act, the Regulation and all other relevant legislation

(b) Other councils or partner organisations such as the NHS. We will advise data subjects should we share their data in this way with third parties;

(c) Disclosures to another third party organisation may be made under an external data sharing agreement. Disclosures from one council department to another will similarly be governed by an internal data sharing agreement.

14.3

In some cases, we may be under a duty to disclose or share a data subject's personal data in order to comply with a legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, or others. This includes exchanging information with other organisations for the purposes of fraud prevention and credit risk reduction.

15. DEALING WITH SUBJECT ACCESS REQUESTS AND BREACHES

15.1

Data subjects must make a formal request for information we hold about them. Wherever possible this should be made via the online form on the Bristol City Council website. Employees who receive a written request must forward it to the Customer Relations Team, Customer Relations (100TS), PO Box 3176, Bristol, BS3 9FS, subjectaccessrequest@bristol.gov.uk) immediately. This request will be completed within 30 days of notification (subject to the content of the request).

15.2

When receiving enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the applicant's identity to make sure that information is only given to a person who is entitled to it.

(b) We will request further information from the applicant where their identity cannot be determined upon the initial

application.

15.3

Subject Access Requests will be dealt with and processed in accordance with the Councils Subject Access Request Policy.

15.4

Data Breaches will be processed in line with current data breach notification procedures. The ICO will need to be notified of any significant data breaches within 72 hours. These will at first instance be logged with the ICT service desk.

16. CHANGES TO THIS POLICY

16.1

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail, email or via our website.

The above is a very broad description of the way Bristol City Council processes personal information. To understand how an individual data subjects personal information is processed they may need to refer to any personal communications they have received including any privacy notice given, or contact the BCC directly to ask about their own personal circumstances.