Data Protection Policy

Version: 2.4

Contents

1 Policy

The types of personal data that BCC may be required to handle include personal information about current, past, and prospective citizens, 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 combined data protection laws (UK General Data Protection Regulations, the Data Protection Act 2018) and other regulations related to personal data.

We must ensure that when processing personal data that:

- The **7 Principles** under UKGDPR are met (processed fairly, lawfully, and transparently, purpose limitation, data minimisation, accuracy, storage limitation, processed with integrity & confidentiality and accountability).
- The correct **Lawful Basis** has been identified to process the personal data (Consent, Contract, Legal Obligation, Vital Interest, Public Interest/Task & Legitimate Interest)
- Have the required documentation in place to protect the personal data of individuals we process:
    - **Privacy Notices (PN)** to be provided no later than 30 days from commencement of processing an individual's data.
    - **Data Protection Impact Assessments (DPIA)** to be carried out prior to any new process/use of new technology where highly sensitive and/or large volume of personal data is to be processed and/or where automatic decision AI is used.
    - **Data Sharing Agreements (DSA)** where data is being shared between one or more data controller.
    - **Internal Data Sharing Records (ISDR)** where data is being shared between different service areas within BCC.
    - **Data Processing Agreement (DPA)** where data is shared to a supplier (Data Processor) who is employed by BCC to process our data on our behalf.
    - **Record of Processing Activity (ROPA)**
    - **Document Retention Schedule (DRS)** all processing of personal data must have a defined retention period recorded on the DRS.
- Accessible when a data subject submits.
    - Data subject access requests (SAR)
    - Individual Rights requests
- Any data that is to be transferred outside of the UK must ensure that the recipient country has the adequate safeguards in place to keep the data safe.
- All data breaches (even if they are suspected) are reported to the data protection team immediately.

- All staff must complete all mandatory training annually as required to ensure that they are fully equipped to manage and process personal data.
- Employees of BCC are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

A copy of the full Data Protection policy is available on request.

2 Definitions

- **Data** is information, which is stored electronically (including mobile devices), on a computer, or in certain paper- based filing systems.

- **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.

- **Personal data** means any information relating to an identified or identifiable natural (living) 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 identify 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.

- **Data controllers** are the organisation, person, agency, or other body that determines and controls 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. Bristol City Council is the data controller for the personal information we process where BCC decides the purposes and means of the processing.

- **Data users** are those of our employees whose work involves processing personal data. They work on behalf of BCC (the data controller).

- **Data processors** act on behalf of, and only on the instructions of the data controller. They have no purpose of their own for processing the data. They include any person or organisation that is not employed by BCC that processes personal data on our behalf and on our instructions. For example, suppliers which handle personal data on BCCs behalf and third parties that may provide technical support.

- **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.

- **Special category data** is information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sex life or sexual orientation, or any genetic or biometric data.

- **Criminal offence data** is information about criminal convictions and offences, or related security measures, which includes information about criminal allegations, proceedings, or convictions.

- **Encryption** - The process of encoding a message or information in such a way that only authorised parties can access it.

- **Confidential Information** - Information provided in confidence by an individual, that they would expect to not be shared further without their consent or a suitable exemption. This includes medical information, demographic information, and information about 3rd parties.

- **Information Commissioner's Office (ICO)** is the independent regulatory office in charge of upholding information rights in the interest of the public. If an organisation fails to adhere to data protection regulations the ICO has the power to enact criminal prosecution and non-criminal enforcement, including fines.

A full list of key data protection terms can be found in the Data Protection Policies Glossary

3 Standards

UK General Data Protection Regulation 2018

Data Protection Act 2018

4 Version Awareness:

Please note that documents printed or downloaded are uncontrolled documents and therefore may not be the latest version.

Ensure this is the latest version by checking Data protection policy (bristol.gov.uk).

Document History		
Version	**Date**	**Details**
1.00	23/10/2018	Draft Document created
2.0	05/06/2020	Full Review and updated drafted
2.1	12/10/2021	Full Review and updated drafted
2.2	31/05/2022	Full Review and updated drafted
2.3	02/07/2023	Full Review and updated drafted
2.4	11/11/2024	Full Review and updated drafted