Data Protection Policy

Version: 2.2

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 the Information Security Source page. Those within the scope of this document are responsible for familiarising themselves periodically with the latest version.

Title:	Data Protection Policy
Description:	Policy setting out Bristol City Council's data protection obligations.
Author:	Natasha Casling
Scope:	All members of staff, visitors or third-party providers of services or support.
Document Status:	Draft
Version	2.2
Classification:	Official
Create Date:	05/06/2020
Approval Body:	Information Governance Board
Date Approved:	02/09/2020 Revision Approved 02/11/2021
Document Review Period:	6 months from approval and annually thereafter unless a significant change is required.
Disposal Period:	Permanent
Security Standard and Clauses **ISO27001:2013 requirements: A.8.1.3, A.13.2.3 and A.18.1.4**	
Document History	

Version	Date	Editor	Details
1.00	23/10/2018	L Miller	Draft Document created
2.0	05/06/2020	K Hygate/B Hodge	Full Review and updated drafted
2.1	12/10/2021	N Casling	Review and update to new UK GDPR regime – all links updated
2.2	31/05/2022	N Casling	Update on Links, full review of content for internal use

Contents

1.0 Purpose of this Policy

1.1. This Policy details what is expected of the organisation and each employee within the organisation to ensure that personal data is respected and managed in line with the combined data protection laws (UK GDPR & DPA 2018) and is always kept secure and only used for the purpose in which It was collected.

1.2. 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 or provided by data subjects, or other sources

2.0 R.A.C.I. Model

2.1. The RACI model is used for clarifying and defining roles and responsibilities in cross-functional or departmental projects and processes as detailed below:

- **Responsible**: All staff, or third-party providers of services or support who use Bristol City Council information assets.
- **Accountable:** Head of Information Assurance.
- **Consult:** Information Governance Board.
- **Inform**: All staff, or third-party providers of services or support who use Bristol City Council information assets.

3.0 Introduction

3.1. Bristol City Council (BCC) is committed to using people's personal data properly and legally, to ensure it is used only in ways people would reasonably expect and that it stays safe. Everyone has rights with regards to the way in which their personal data is handled. During our activities we collect, store and process personal data about our citizens, service users, employees, suppliers and other third parties. We recognise that the correct and lawful treatment of this data maintains trust and confidence in the organisation and provides for successful service delivery.

3.2. Employees of BCC are obliged to comply with the Combined Data Protection Laws (UK GDPR & Data Protection Act 2018) when processing personal data on our behalf. A breach of either the Data Protection Act 2018 or UK GDPR (UK General Data Protection Regulation) may result in criminal proceedings and may result in disciplinary action which could result in dismissal.

3.3. 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.

4.0 Definitions

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

4.2. **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.

4.3. **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.

4.4. **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.

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

4.6 **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.

4.7 **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.

4.8 **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.

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

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

4.11 **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.

4.12 **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

5.0 Data Protection Principles & Lawful Basis

5.1. BCC is required to process personal data in accordance with seven key principles. Personal data must be:

(a) Processed fairly, lawfully, and transparently.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

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

(d) Accurate and where necessary, kept up to date.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

(f) Processed in a manner that ensures appropriate security of the personal data.

And BCC is required to:

(g) Take responsibility for what we do with personal data and how we comply with these other principles and be able to demonstrate our compliance.

5.2 Personal data can only be processed if there is a valid lawful basis for processing. There are six lawful bases:

(a) Consent – a person has given clear consent to process their data for a specific purpose.

(b) Contract – processing is necessary to perform a contract with a person or because they have asked for specific steps to be taken prior to entering into a contract.

(c) Legal obligation – the processing is necessary to comply with the law.

(d) Vital interests – the processing is necessary to protect someone's life.

(e) Public task – the processing is necessary to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests (this cannot apply to BCC processing data to perform its official tasks)

5.3. When **special category data** is processed, the lawful basis for processing must be identified and in addition can only be processed if a further separate specified condition for processing is identified.

5.4. When **criminal offence data** is processed, the lawful basis for processing must be identified and in addition can only be processed when either legal authority or official authority for the processing is identified.

5.5. The lawful bases BCC relies upon when we carry **out automated decision making, and profiling** are public task and legitimate interests. The information we are required to give to data subjects in relation to automated decision making and profiling is stated in the relevant privacy notices.

6.0 Documentation of Processing

6.1 When processing personal data as data controller, BCC will ensure that the lawful bases for processing and the additional conditions for processing when required are identified and documented in the record of processing activity (ROPA).

At a minimum, the ROPA also documents:

- Name and contact details of BCC
- Purposes of processing
- Categories of data subjects and categories of personal data
- Categories of recipients of personal data
- Details of transfers to third countries and the transfer mechanism safeguards in place including an indication for the legal basis for the processing of the personal data, (including transfers).
- Retention schedules
- Technical and organisational security measures
- Details the use of automated decision-making and profiling.

6.2 BCC considers how the processing may affect individuals concerned and can justify any adverse impact. Personal data is only processed in ways individuals would reasonably expect. If this is not the case, BCC can explain why any unexpected processing is justified.

6.3 BCC is open and honest about its processing of personal data and ensures that people have the information required about the collection and use of their personal data. This is provided by way of privacy notices.

6.4 BCC maintains 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 data protection impact assessment (DPIA) for all processing that is considered to be high risk, in accordance with the Data Protection Impact Assessment Policy

7.0 Processing of Personal Data for Limited Purposes Only

7.1. BCC is required to be clear and open about the reasons for obtaining and processing data. When processing personal data as data controller, BCC:

(a) records the purposes for processing personal data in the ROPA and specifies them in the privacy notice provided to individuals,

(b) only collects the minimum amount of personal data, which is actually needed for the specified purposes,

(c) only uses the personal data for a new purpose if it is compatible with the original purpose or consent is given or there is a clear obligation or function set out in law,

(d) Regularly reviews the purposes for processing and when necessary, updates the ROPAs and privacy notices.

8.0 INFORMATION PROVIDED TO DATA SUBJECTS

8.1. BCC provides individuals with the following privacy information in our privacy notices, in relation to the collection and use of their personal data.

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

(b) The purposes of the processing

(c) The lawful bases for the processing

(d) The legitimate interests for the processing (if applicable)

(e) The categories of personal data obtained (if the personal data is not obtained from the data subject it relates to)

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

(g) Details of transfers of the personal data to any third countries or international organisations (if applicable)

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

(i) The rights available to data subjects in respect of the processing including the right to withdraw consent (if applicable) and the right to lodge a complaint with Information Commissioner's Office (ICO)

(j) The source of the personal data (if the personal data is not obtained from the data subject it relates to)

(k) Details of whether data subjects are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the data subject it relates to)

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

8.2 This privacy information is provided to data subjects at the time we collect their personal data from them.

When their personal data is obtained from another source, we provide this privacy information:

- within no later than one month of obtaining the personal data.
- if we plan to communicate with the data subject, at the latest when the first communication with the data subject takes place; or
- if we plan to disclose the data to someone else, at the latest, when the personal data is disclosed.

9.0 Data Minimisation and Accuracy of Personal Data

9.1 BCC only collects the personal data we need for our specified purposes and ensures we have sufficient data to properly fulfil those purposes. We take steps to truly anonymise data where possible. We periodically review the data we hold and delete anything we do not need in line with the data retention policy.

9.2 BCC takes steps to truly anonymise data where possible, stripping the personal data of sufficient elements meaning the data subject cannot be identified and it is no longer personal data. BCC recognises that if there are reasonably available means to re-identify the data subject, this is not true anonymization and the data remains personal data, subject to data protection legislation.

9.3 BCC takes all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact. We take all reasonable steps to keep the personal data updated and correct or erase personal date if we discover it is incorrect or misleading. We carefully consider any challenges to the accuracy of personal data.

10.0 Retention of Personal Data

10.1 BCC holds personal data in accordance with the standard retention periods found in the document retention schedule and in line with the data retention policy.

10.2 BCC only keeps personal data for as long as is necessary for the purposes for which it was collected. We take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. Any personal data we need to keep for public interest archiving, scientific or historical research, or statistical purposes is clearly identified.

11.0 KEEPING PERSONAL DATA SECURE

11.1 BCC processes all personal data we hold in accordance with our information security policies.

11.2 BCC ensures there are appropriate security measures in place to maintain the security of all personal data from the point of collection to the point of destruction.

11.3 We 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.

11.4 Security procedures include but are not limited to:

(a) Access controls. Any stranger seen in access-controlled areas should be reported. All BCC employees should have their employee ID card on them at all times when within BCC property.

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

(c) Files securely stored. Files are securely stored at a B Bond and managed by the Modern Records Unit. Only permitted personnel are allowed to request files stored.

(d) Methods of disposal. Paper documents should be disposed of in confidential waste sacks or shredded. Digital storage devices should be physically destroyed when they are no longer required or sanitised in accordance with the information security policies. Disposal of data should be recorded.

(e) 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.

(f) Information security policy: All employees must have read and apply the provisions of the Acceptable Use Policy.

(g) Training: All employees including casual employees and contractors must complete information security and data protection training before being allowed access to BCC network. Such training must be confirmed on employee's appraisals 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 and that additional data protection training needs are identified, and relevant training complete to ensure employees are able to process personal data securely and lawfully.

12.0 Transferring Personal Data to A Country Outside the EEA

12.1 BCC may only transfer any personal data we hold to a third party outside the European Economic Area ("EEA") if the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms or an appropriate safeguard is in place between BCC and the third party. If this is not the case, a transfer can only be made if it is covered by an exception. Such transfers are made in line with the data sharing policy and accompanying procedures.

13.0 Disclosure and Sharing of Personal Data

13.1 BCC may share personal data we hold across council services in accordance with the privacy notices provided to data subjects, either at the point of initial contact or via our website. Disclosures from one council department to another are recorded in an internal data sharing record.

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

(a) Contractors or suppliers **(data processors)** who work for us to deliver our services. A contract must be in place with all data processors, which is compliant with data protection 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. Any disclosure to another council or partner organisation must be made under an external data sharing agreement in line with the external data sharing protocol and data sharing policy.

13.3 In some cases, BCC 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. Such disclosures are made in line with the relevant policies and procedures.

14.0 Processing of Personal Data in Line with Data Subject's Rights

14.1 BCC will process all personal data in line with data subjects' rights, including their rights to:

(a) be informed about the collection and use of their personal data,

(b) access their personal data,

(c) have inaccurate data amended or completed,

(d) have personal data erased,

(e) request the restriction of suppression of their personal data,

(f) move, copy, or transfer personal data easily from one database to another or organisation safely and securely without hindrance to usability,

(g) object to the processing of their personal data in certain circumstances and their absolute right to stop their data being used for direct-marketing purposes,

(h) object to profiling and other rights in relation to automated decision making.

15.0 Dealing with Subject Access Requests, Other Data Subject Requests and Data Breaches

Data subject requests, including subject access requests

15.1 All **subject access requests** will be dealt with in accordance with the subject access request policy and procedures.

15.2 Data subjects are able to make a **request to exercise their rights** under the Act, including a request to access a copy of the personal data BCC holds about them as well as other supplementary information (known as an individual rights request). Data subject requests can be made formally or informally, in writing or verbally. Wherever possible, a subject access request should be made via the online form on the BCC website.

15.3 BCC will comply with requests within one calendar month of receipt or (if later) within one calendar month of receipt of any information requested to confirm the requester's identity or a fee if applicable. In certain circumstances it is possible to extend the time to respond by a further two months.

15.4 When receiving data subject requests, we will only respond to these requests, including disclosing, amending, or erasing personal data if the following conditions are met:

(a) We are satisfied as to the identity and/or authority of the requester.
(b) We request and receive further information from the requester where their identity and/or authority cannot be determined upon the initial application.
(c) We have received sufficient information from the requester to locate the relevant data.

Data Breaches

15.5

(a) A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This can be either accidental or deliberate.

(b) All staff have a duty to report a confirmed or suspected personal data breach via the internal reporting process as soon as they become aware. The Statutory Data Protection officer is responsible for investigating the breach and if necessary, notifying the ICO within 72 hours of becoming aware of the breach and the individuals concerned without undue delay. BCC keeps a log of all data breaches. All data breaches are processed in line with the data breach policy and procedures.

16.0 Governance and Responsibilities

16.1 Bristol City Council is the data controller for the personal information we process. Our main office is based at City Hall, College Green, and Bristol, BS1 5TR our contact details can be found on the BCC Website.

16.2 This policy is approved by the Information Governance Board of the BCC. 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. The Information Governance Board is accountable to the Corporate Leadership Board which holds overall responsibility for compliance with data protection obligations.

16.3 The Senior Information Risk Officer (SIRO) has overall responsibility for information risk at all levels of BCC and leads the Information Governance structure.

16.4 The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information and ensuring it is used properly.

16.5 The Data Protection Officer (DPO) is responsible for assisting BCC to monitor internal compliance with data protection legislation and this policy, advising on data protection obligations, providing advice and monitoring data protection impact assessments. The DPO acts as a contact point for data subjects and the Information Commissioner's Office. 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 3399 Bristol, BS1 9NE, Data.protection@bristol.gov.uk

16.6 Information Asset Owners are responsible for the processing of personal data within their teams/directorates/service area. This includes:

- Making decisions about value, risks, and resources in relation to the processing of personal data.
- Approving data quality targets authorise data sharing agreements and contracts.
- Maintaining an accurate and up to date record of processing activities (ROPA).
- Ensuring data protection impact assessments (DPIAs) are conducted when required.
- Ensuring that privacy notices are in place, up to date and provided to data subjects at the right time.
- Ensuring that data subject requests, including subject access requests are recognised and responded to in accordance with policies and procedures.
- Working to reduce the risk of data breaches occurring, and when they do occur, ensuring that breaches are recognised and reported in line with policies and procedures.

16.7 Lead Custodians are responsible for helping to define data quality and data standards, helping to mitigate risks in relation to processing personal data and are responsible for managing personal data to a defined quality.

16.8 The Information Governance service is responsible for providing advice, support, and co-ordination in relation to data protection to the Information Asset Owners, the Lead Custodians, the Caldicott Guardian, the Senior Information Risk Owner and the Data Protection Officer.

16.9 All employees are responsible for protecting and processing the personal data they handle in accordance with this data protection policy, other related data protection procedures and the relevant legislation at all times - including abiding by the employee code of conduct

16.10 This policy is approved annually by the Information Governance Board. BCC reserves the right to change this policy at any time. Where appropriate, we will notify data subjects of any changes by mail, email or via our website.

17.0 Risks

It is important to ensure that the details outlined in this Policy are understood and followed to prevent any risks in the management of individuals personal data and that all risks are considered in the processing of an individual's data.

Failure to adhere to the Policy poses financial and reputation risks to Bristol City Council. Fines up to 4% of Bristol City Council's turnover may be imposed by the ICO. This will result in a huge financial impact to the Council being able to offer its citizens with the services they require.

The risk to employees is that not following the details as outlined in this Policy could result in action taken against the employee which could result in dismissal or action being taken by the ICO against them – this could be fines and/or court action.

18.0 Summary

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:

- Processing must be Fair, transparent, and lawful
- Be only collected for the purpose required (Purpose Limitation)
- Personal data must only be collected that meets the requirements and nothing more (Data Minimisation)
- Personal data must be accurate (Accuracy)
- Personal data must be kept secure even when our systems our at rest (Integrity & Confidential)
- Personal data must only be kept for the time it is necessary and therefore have clear retention times and processes in place to manage the retention of information (Storage Limitation)
- Have the required documentation in place to protect the personal data of individuals we process
    - Privacy Notices (PN)
    - Data Protection Impact Assessments (DPIA)

  - Data Sharing Agreements (DSA)
  - Record of Processing Activity (ROPA)
- 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.
- Report all data breaches (even if they are suspected) to data protection team immediately
- All staff must complete all training required to ensure that they are fully equipped to manage and process personal data.

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

Standards

UK General Data Protection Regulation 2018
Data Protection Act 2018

Further Information

For further information please email data.protection@bristol.gov.uk