Data Sharing Policy

Version: 2.01

Contents

1. Policy Summary

BCC's suite of Information Security Policies held on Metacompliance set out BCC's obligations in relation to the security of personal data.

This policy sets out BCC's obligations in relation to sharing of personal data, as set out in in the ICO's Data Sharing Code of Practice. Documenting our data sharing agreements ensures that we meet the UK GDPR principles of lawfulness, fairness, and transparency (Art 5(1)(a)), accountability (Art 5(2)) and that we have a lawful basis to share information (Art 6).

This policy does not relate to sharing of data with Data Processors. Sharing of Data to our Processors is covered in the Data Processing Agreements held between BCC and the Processor.

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we collect, store and process personal data including sharing some of the 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.

A data sharing agreement (personal data shared between two or more Data Controllers) provides a framework to help you meet the requirements of the data protection principles.

Where data is to be shared with another department, service area or an external organisation a data sharing record (internal sharing) or data sharing agreement (external sharing) must be put in place before any data is shared.

Where information is shared with the police, other local authorities, and other external agencies a Schedule 2 must be received and details of the reasons why the information is required is provided. Where data is regularly shared with other government departments (Police, NHS for instance) A Tier 1 may be created with defined details of data sharing detailed in Tier 2's and where we are to share information with central government, we may enter into a memorandum of understanding with each other that includes data sharing provisions and fulfils the role of a data sharing agreement.

The risks of sharing the data must be identified and actions (mitigations/countermeasures) are put in place to ensure that the safe sharing of the data is maintained at all times.

All methods of data sharing records/agreements should be reviewed by data protection team.

Where the sharing of data could cause high risks to individuals (for example, automated decision making, new technology for transferring of data, sensitive data, data relating to vulnerable adults, matching of databases, large volumes of data subjects etc) a DPIA Pre

Screener (data protection impact assessment) must be submitted to data protection for review.

A data sharing agreement between the parties sending and receiving data can form a major part of our compliance with the accountability principle.

A Data Sharing agreement:

- Helps all the parties be clear about their roles.
- Sets out the purposes of the data sharing.
- Covers what happens to the data at each stage; and
- Sets the Standards of each party within the agreement.
- Managing the parties obligations one to the other.

All data sharing agreement templates must be requested from data protection to ensure the correct version is used.

Signed data sharing records and agreements must be registered with the Information Governance service by sending a copy of the signed agreement/record to data.protection@bristol.gov.uk.

It is the responsibility of the data owner to ensure that any data sharing between either external parties or internal parties where systematic sharing of data is to take place has a suitable data sharing agreement or internal sharing record is in place and that the process is entered onto the ROPA and referenced in the Services Privacy Notice.

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

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

3 Definitions

3.1 **Data Subject** – The Data Subject is the living individual to whom the data requested in the SAR relates.

3.2 **Data controller** - 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.

3.3 **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 and third parties that may provide technical support.

3.4 **iCasework** – The case management software used by BCC to manage SARs.

3.5 **Personal data** - Personal data means any information relating to an identifiable person who can be directly or indirectly identified from it. This can include an IP address or other online identifier as well as the more obvious name, address etc. More information about what constitutes personal data can be found on the ICO website - What is personal data? | ICO

3.6 **Privacy Notice** – This is the notice we must give to a Data Subject at the time we collect their data which explains why we are collecting their data, what data we collect, how we use it, who we share it with, what their privacy rights are and who to complain to.

3.7 **Record of Processing Activity (RoPA)** – Each area of the business must maintain a record of all processing activities it carries out that relates to personal data.

3.8 **Subject Access Request (SAR)** – A request made by or on behalf of a Data Subject to obtain their personal data as processed by BCC.

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

3.10 **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.

3.11 **Schedule 2** – Document to be completed by a senior member of staff of the requesting organisation where a one-off request is received from Police, other authorities, and agencies. This is not the same as a Tier 1 or Tier 2 agreement.

3.12 **Tier 1 or 2 agreements** – a sharing framework (usually organisations like Police & NHS are the lead data controllers of the Tier 1/2 documents) where information is shared amongst multiple authorities and organisations which provides an overarching agreement which sets out the guiding principles and ethos of data sharing between the signatories to this. This is signed off once by or on behalf of a chief officer or equivalent for each organisation. The second tier is the specific agreement between the signatories for the sharing of personal data. When two organisations know exactly what data they want to share, for what purpose and for how long etc. they sign up to a Tier 2 DSA. It can be signed off by local managers, asset owners, asset assistants, asset guardians, asset custodians or anyone who considers themselves accountable for the data and the data exchange.
As the Tier 2 DSA relates to specific sharing of data, an organisation may have multiple Tier 2's in place.

3.13 **Annex C** – document to be completed by the Police/Crown Prosecution when information is requested that relates to a sexual abuse case of an individual who is/was 17 at the time of the alleged crime. This is not the same as a Tier 1/2 or a Schedule 2.

4 Responsibilities

- **Data controller** – The person/organisation who determines either alone or jointly with others on the purpose and means of the processing of personal data.
- **Information Asset Owner (IAO) –** These individuals own the information processed within their service area. They are responsible for addressing risks to the information, ensuring it is accurate, and maximising the value of the information.
- **Lead Custodian** – These individuals manage information processed within their service area. A list of all current IAOs and Lead Custodians can be found on the Source - BCC Information Governance Roles.xlsx (sharepoint.com).
- **Statutory Data Protection Officer (SDPO)** – The SDPO is responsible for monitoring internal compliance with data protection legislation and this policy. The SDPO acts as a contact point for Data Subjects and the ICO. In this document where reference is made to consulting the SDPO, they can be contacted at data.protection@bristol.gov.uk

5 Standards

UK General Data Protection Regulation (UKGDPR)

Data Protection Act 2018 (DPA 2018)

6 Further Information

Police and other agencies request for personal information (bristol.gov.uk)

For further information or a full copy of this policy please email data.protection@bristol.gov.uk

7 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 MetaCompliance - MyCompliance Cloud. Those within the scope of this document are responsible for familiarising themselves periodically with the latest version.

Title:	Data Sharing Policy
Description:	Provides the Council's Policy for sharing of personal data both internal and with external organisations, clearly describing the processes to be taken and the considerations around the sharing of personal data to ensure it is conducted lawfully and transparently
Author:	Data Protection Officer
Scope:	All members of staff
Document Status:	Published
Version:	2.01
Classification:	Official
Create Date:	27.10.2022
Approval Body:	Information Governance Board
Date Last Approved:	19.12.2023

Document Review Period:	6 months from approval and annually thereafter unless a significant change is required.
Next Review Date:	November 2024
Last Reviewed Date:	30.11.2023
Disposal Period:	Permanent

Document History			
Version	**Date**	**Editor**	**Details**
2.00	27/10/2022	N Casling	Upgrading of old Policy for compliance and conversion to MetaCompliance
2.01	30/11/2023	N Casling	Upgrade to new format for ease of reading

8 R.A.C.I. Model

8.1 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.