Bristol City Council
Data Protection Policies

GLOSSARY

Title:	Data Protection Policies: Glossary
Description:	Glossary providing descriptions for key terms contained within BCC's data protection policies
Author:	Kate Hygate
Sponsor:	Ben Hewkin
Document Status:	Signed-off
Version:	2.0
Classification:	OFFICIAL - Public
Creation date:	26/06/2020
Approval body:	BCC Information Governance Service
Date approved:	22/07/2020
Document Review Period:	Annual
Disposal Period:	N/A

Reviewed: 15.11.2022
Updated: 15.11.2022

Introduction

Bristol City Council's data protection policies contain a number of technical terms. The definitions of these terms are found in this glossary, rather than in the body of the policy, other than the Data Protection Policy, which, as the foundational policy, contains definitions of key terms, which are replicated here.

Definitions (listed alphabetically)

Accuracy BCC must take every reasonable step to ensure the data processed is accurate and, where necessary, kept up to date. Reasonable measures should be understood as implementing processes to prevent inaccuracies during the data collection process as well as during the ongoing data processing in relation to the specific use for which the data is processed. BCC must consider the type of data and the specific purposes to maintain the accuracy of personal data in relation to the purpose. Accuracy also embodies the responsibility to respond to data subject requests to correct records that contain incomplete information or misinformation.

Anonymisation is when personal data is stripped of sufficient elements which means that the individual can no longer be identified and cannot in the future be identified. When data has been anonymised, it is no longer subject to data protection legislation.

Automated decision making is the process of making a decision using personal data about an individual without human involvement.

Availability Data is available if it is accessible when needed by BCC or the data subject. BCC is required to ensure the availability of personal data it processes.

Biometrics is data concerning the intrinsic physical or behavioural characteristics of an individual. Examples include DNA, fingerprints, retina and iris patterns, voice, face, handwriting, keystroke technique and gait.

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

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

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.

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.

Data subjects all living individuals about whom we hold or could 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.

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

DPA (Data Protection Agreement) – an agreement which by law is required between a Data Controller and a Data Processor

Data Protection Impact Assessment (DPIA) previously referred to as Privacy Impact Assessment (PIA) is a written assessment that helps BCC identify, evaluate and mitigate risks and privacy impacts to data subjects arising as a result of processing their personal data. A DPIA must be undertaken **before** the processing of any personal data which is 'likely to result in a high risk to the rights and freedoms' of data subjects.

DSA (Data Sharing Agreement) – an agreement that sets out the obligations of data sharing partners one to the other with regard to the sharing of personal data

Information Commissioner's Office (ICO) is the independent regulatory office in the UK who is 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.

Lawful Basis is the term used under the combined data protection laws (UK GDPR & DPA 2018) to describe the lawful grounds for which processing can be carried out. These are Consent, Contract, Legal Obligation, Public Task, Legitimate Interest & Vital Interest.

Legal Gateway is the term used where we are obliged by a public law (statutory power) to process data and is required to be determined if the Lawful Basis of Legal Obligation or Public Task/Interest is quoted e.g., Council Tax (Administration and Enforcement) Regulations 1992, Allotments Act 1950, Local Government Act 1972, Care Act 2014, Mental Health Act 1983 etc

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. More information about what constitutes personal data can be found on the ICO Website.

Privacy Notice is a statement made to data subjects that describes how an organisation collects, uses, retains and discloses personal information.

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.

Profiling is the automated processing (i.e., processing without any human intervention) of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual in such a way that they can no longer be identified without reference to additional information. For example, replacing an easily attributable identifier such as a name with an ID number. Where pseudonymisation is used it is still possible to identify an individual, and as such the data is still personal data for data protection purposes.

ROPA (Record of Processing Activity) is a legal requirement under UK GDPR to record the processes undertaken which involve the collection, storing, processing, and sharing personal data

SAR (Subject Access Request) is the request from an individual for any information that BCC holds about them. Under UK GDPR the data subject shall have the right to obtain from BCC confirmation as to whether or not personal data concerning them are being processed and to have that information provided to them.

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.

UK GDPR (UK General Data Protection Regulation) protects the fundamental rights and freedoms of natural persons (living individuals) and in particular their right to the protection of personal data. Implemented in May 2018 as GDPR, however with the exit of the UK from Europe it is now known as UK GDPR.