Data Breach Policy

Version: 1.4

Version Awareness:

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

Title:	**BCC Data Breach Policy**
Description:	Policy for detecting and responding to personal data breach occurrences at Bristol City Council
Author:	Data Protection Officer
Sponsor:	Head of Service
Scope:	All members of staff, visitors or third-party providers of services or support
Document Status:	Draft
Version:	1.4
Classification:	Official - Public
Create Date:	05/06/2020
Approval Body:	Information Governance Board
Date Approved:	02/09/2020
Document Review Period:	Annually
Disposal Period:	Permanent
Security Standard and Clauses **ISO27001:2013 requirements: A.8.1.3, A.13.2.3 and A.18.1.4**	

Version	Date	Details
1.04	21.06.2022	Update of format to current version and to reflect that UK GDPR is now the data protection legislation

Contents

1 Purpose of this Policy

The combined data protection laws (UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018)) regulate the processing of 'personal data'. Data protection legislation contains data protection principles which must be complied with when processing personal data.

BCC's Information security policy statement (bristol.gov.uk) set out BCC's obligations in relation to the security of personal data.

This policy sets out BCC's obligations in relation to data breaches, as set out in Articles 33 and 34 of the UK GDPR and Part 3 Chapter 4 of the DPA 2018.

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

Data Processors acting on the instructions of BCC are obliged to comply with this policy when processing personal data on our behalf, as detailed in the contract between BCC and the processor.

The full details of the Policy are contained in the following pages. It provides the details about BCC's obligations and how it complies with them when processing personal data.

2 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 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 regard to the way in which their personal data in handled. During

the course of 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.

4 Definitions

- **IAO – Information Asset Owners** are responsible for the processing of personal data within their service area.

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

5 Responsibilities

- **Data controller** – BCC is the data controller.
- **Information Governance Board** – This policy is approved by the IGB, who lead and advise on data protection within BCC. This policy is periodically reviewed by the IGB.
- **Data Protection Officer (DPO)** – is responsible for assisting BCC to monitor internal compliance with data protection legislation and this policy. The DPO acts as a contact point for data subjects and the Information Commissioners Office. In this document where reference is made to consulting the DPO, they can be contacted at data.protection@bristol.gov.uk
- **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 and the DPO.
- **Data Protection Team** – is a part of the information governance service. In relation to data breaches, it is responsible for assisting the DPO to monitor and support BCC's compliance with its data breach duties as set out in data protection legislation.
- **Information Asset Owners –** are responsible for the processing of personal data within their service area. This includes working to reduce the risk of data breaches occurring and ensuring that all data breaches are recognised, responded to and reported in line with this policy and procedure.
- **Lead Custodians** – in relation to data breaches, they are responsible for supporting the IAO to ensure all data breaches are recognised, responded to and reported in line with this policy within their service area, and working to reduce the risk of data breaches occurring.
    - **All staff** are responsible for recognizing and reporting data breaches when they occur and for ensuring they ask for training or help to be able to do this.

6 Policy Statement and Provisions

6.1 What is a personal data breach?

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

  Common examples of data breaches include:

  - personal data being sent to someone (internally or externally) who is not authorised to see it,
  - records being deleted accidentally,
  - paper records containing personal data being left on desks, in meeting rooms, at photocopiers and not properly disposed of, to be copied, read or photographed by an unauthorised person,
  - personal data being recorded in someone else's record by accident,
  - sharing of passwords or other credentials with third parties,
  - loss or theft of devices containing personal data,
  - unlawful interception of email or telephone communications or online form submissions,
  - being tricked by a third party into releasing personal data of another person,
  - loss of personal data due to fire or flood,
  - a ransomware attack whereby access to systems or records containing personal data is disabled or encrypted,
  - a cybersecurity attack whereby personal data is accessed, deleted and/or disclosed by the attacker.

6.2 Duties in relation to personal data breaches

- BCC is required to:

  (a) keep a record of all personal data breaches that occur in relation to data which is being processed by BCC or on its behalf by a data processor,

  (b) report personal data breaches which are likely to impact individuals' rights and freedoms to the ICO within 72 hours of discovery of the breach where feasible,

  (c) inform data subjects of the breach without undue delay if the breach is likely to result in a high risk of adversely affecting their rights and freedoms.

Failure to notify the ICO of a personal data breach when required to do so can result in a fine of up to £8.7 million or 2% of turnover.

- The internal breach detection, investigation and internal reporting procedures outlined below are in place to enable BCC to meet these duties.

- All staff are obliged to comply with BCC's Information Security Incident Reporting Policy in order to minimise the likelihood of data breaches occurring and work with their managers who ensure staff undertake annual mandatory and refresher data protection training so that they are able to recognise a data breach and know how to report it. Staff are assured that reporting of any potential personal data breach will not result in suffering any detrimental treatment as a result of raising their concerns.

- Additionally, BCC holds a separate 'Caldicott Log' which records all breaches involving health and social care personal data. This is maintained by the Information Governance service.

6.3 Duties of data processors in relation to personal data breaches.

- Data processors are required to inform BCC as soon as they become aware that a breach has occurred. As data controller, it is BCC's responsibility to address the breach and report to the ICO and notify the data subjects if necessary. This duty is detailed in all contracts between BCC and data processors.

7. Risks

- Exposure to risks to both individuals and the organisation if data management and security measures are not put in place
- Non reporting of breaches puts the Council and its service users at risks of continued potential reputational, emotional, and financial or physical harm.
- Fines applied by the ICO which could be £8,700,000 or 2% of our total annual turnover of the preceding financial year, whichever is highest for the following:
    - for not having in place a policy and processes to identify, manage, report and mitigate future data breached.
    - Failure to notify the ICO of a personal data breach when required to do so can also incur fines.
- Reputational damage to BCC, lack of trust from all data subjects on the safe handling of their personal data.

- Suspension of our processing until such times the breach has been identified and corrected, potentially causing loss of services to our citizens, financial loss due to the inability to collect monies due to the Council
- Loss of monies due to the data breach being against our financial accounts.
- Any person who has suffered material or non-material damage as a result of a breach has the right to compensation. They have the right to submit their case through the Courts.

8. Summary

- A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach can be either accidental or deliberate.
- All personal data breaches must be recorded, investigated whether processed by BCC (the Data Controller) or by a Processor working on behalf of BCC
- Data processors are required to inform BCC as soon as they become aware that a breach has occurred. As data controller, it is BCC's responsibility to address the breach and report to the ICO and notify the data subjects if necessary. This duty is detailed in all contracts between BCC and data processors
- Where personal data breaches have been identified by data protection as a high risk to the data subject and therefore will impact the individual's rights and freedoms, they must be reported to the ICO within 72 hours and the data subjects informed.
- All personnel and contractors or anyone who has access to our systems must undertake the Mandatory security training on commencement of employment and complete annual refresher courses
- BCC holds a separate 'Caldicott Log' which records all breaches involving health and social care personal data. This is maintained by the Information Governance service
- Failure to notify the ICO of a personal data breach when required to do so can result in a fine of up to £8,700,000 or 2% of turnover.
- Failure to comply with this Policy is a breach of this policy and may result in disciplinary action being considered which may result in dismissal

9. Standards

UK General Data Protection Regulation

Data Protection Act 2018

10. Changes to this policy

This policy is reviewed at least annually and approved by the Information Governance service. BCC reserves the right to change this policy at any time