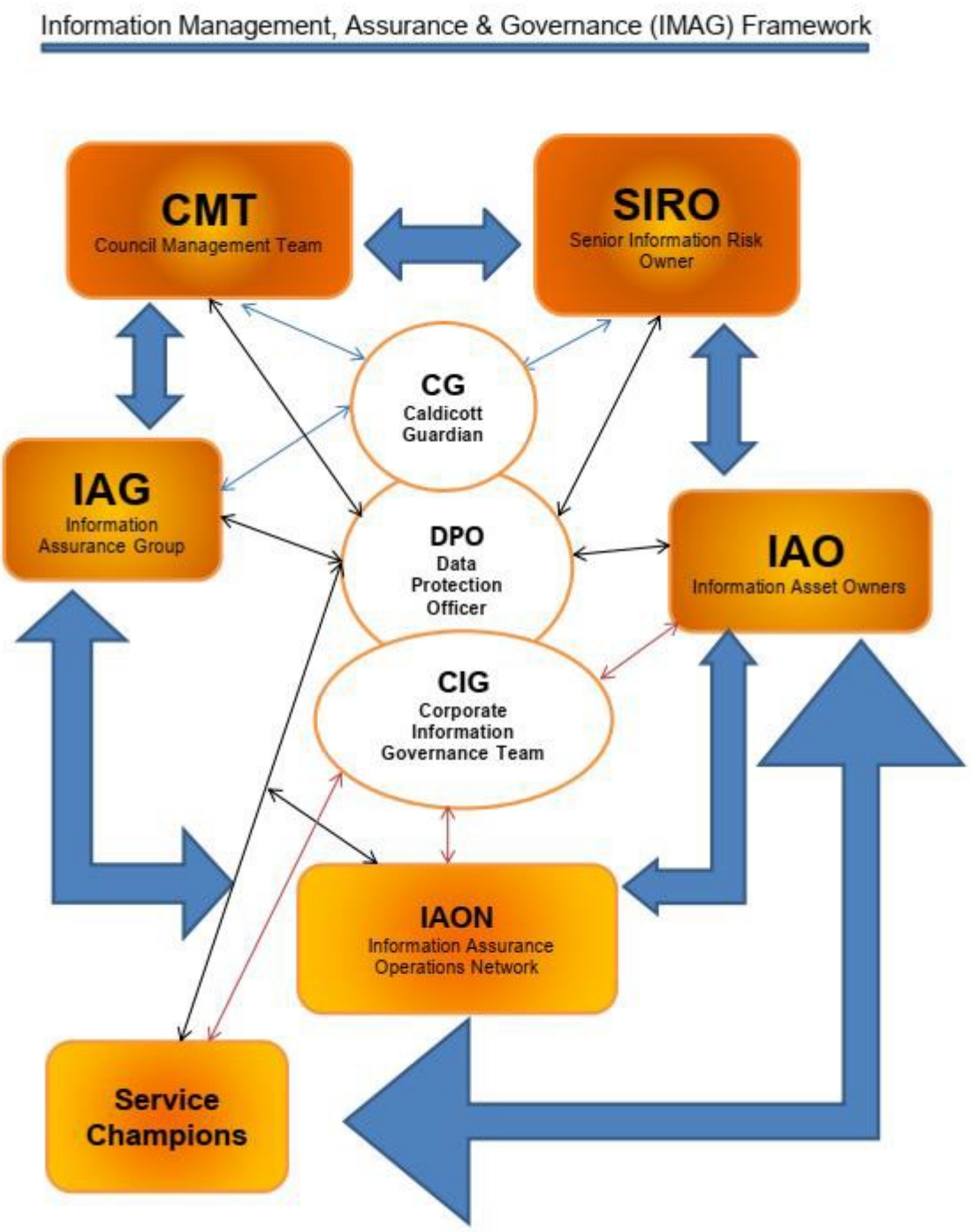
City of BRADFORD METROPOLITAN DISTRICT COUNCIL

City of Bradford Metropolitan District Council

Data Protection Policy

Date Reviewed:	April 2021
Reviewed By:	Corporate Information Governance
Version Control:	v6.0 FINAL
To be reviewed:	April 2023 (subject to changes in Legislation)
Owner:	Corporate Information Governance

Contents



Introduction

All Council Employees managing and handling personal information need to understand their responsibilities in complying with the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR). The DPA and UK GDPR came into effect on 25 May 2018. These two Acts govern the collection, retention, processing and transmission of information held about living individuals along with the rights of those individuals granted in the legislation (Data Subject Rights see Section 4).

Employees must be aware of the potentially far-reaching effects of this legislation. Those that record and use personal information are required to follow seven key Data Protection Principles as detailed in Section 3 of this policy. They should also be aware of the eight Data Subject Rights as detailed in Section 4 of this policy.

Scope

This policy applies to:

- all permanent and temporary employees of Bradford MDC
- any individual including contractors, volunteers and others who work on behalf of the Council
- all apprentice/ work experience and other students
- Elected Members

This policy outlines the behaviours and responsibilities expected in order to ensure the Council continues to fulfil its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018 and their related and all subsequent Data Protection legislation.

Data Protection Principles

At the core of both the DPA and UK GDPR are seven Data Protection Principles set out under Article 5 of the UK GDPR, and section 86 DPA 2018. Any employee who record and use personal information are required to follow seven key Data Protection Principles.

In particular, personal data must:

Lawfulness, fairness and transparency: Be processed lawfully, fairly and transparently.

Purpose limitation: Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data minimisation: Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy: Be accurate and where necessary kept up to date. Inaccurate data, having regard to the purposes for which they are processed must be erased or rectified without delay.

Storage limitation: Personal data must not be kept for any longer than is necessary for the purpose for which it is processed.

Integrity and confidentiality (security): Be protected using appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of the data.

Accountability: The controller shall be responsible and be able to demonstrate compliance with the aforementioned principles.

The legislation is not limited specifically to data held electronically: it applies to all personal information, as long as the data is in a system that allows the information to be readily accessible. Under the UK GDPR and DPA, the processing of information includes any activity concerning the data involved such as altering or deleting it, downloading, reviewing or transferring it. The UK GDPR extends the rights of individuals, as well as requiring the use of appropriate security measures for the protection of personal data. Special treatment is required for the processing of "special category data" (e.g. religion, ethnicity, health etc.).

Separate guidance covering definitions and specific procedures can be found under Data Protection Guidelines.

Data Subject Rights

The UK GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Employee responsibility

All employees **must** ensure that they:

- complete the mandatory minimum standard of Information Security and the UK GDPR eLearning every 12 months and have this recorded in Evolve.
- comply with the seven Data Protection Principles, as listed in the UK GDPR (and summarised in Section 3 of this policy).
- ensure that Data Subject Rights, as defined in the UK GDPR (and summarised in Section 4 of this policy) are appropriately exercised and that they respond to any Subject Access Requests received either verbally or in writing within the statutory one-month requirement.

- regularly review data protection procedures and guidelines within the organisation.
- keep their personal employment data accurate and up to date.
- report any personal data breaches they cause or discover to their line manager and ensure that the incident is reported to the Corporate Information Governance Team using the online Data Security Incident (DSI) form.
- When emailing personal and sensitive information that it is sent securely using GalaxKey.

Offences under the UK GDPR and DPA

Failure to comply with the legislation can result in the Council being fined up to £17.5 million as well as presenting a reputational risk for the Council. Additionally, the Council may also be subject to pay compensation to individuals whose data has not been handled in accordance with the legislation.

Failure to observe the data protection standards set out in this policy maybe regarded as serious and any breach may render an employee liable and subject to disciplinary action.

Additional Policies/Procedures

Records Management Policy

Handling Data Subject Requests Policy

Freedom of Information Act & Environment Information Regulations Policy

Data Security Incident Policy

ICO Data Sharing Code of Practice

Additional legislation to consider

Human Rights Act 1998

The Regulations of Investigatory Powers Act 2000

The Freedom of Information Act 2000

Environmental Information Regulations Act 2004

Privacy Electronic Communication Regulations Act 2003

The Computer Misuse Act 1990

The Public Interest Disclosure Act 1998

Useful contacts

Corporate Information Governance team via foi@bradford.gov.uk

Data Protection Officer via dpo@bradford.gov.uk

Information Commissioner's Office via www.ico.org.uk