Data Protection Policy

1. Purpose

This policy outlines the standards expected of all Brighton & Hove City Council employees, and any third parties, when processing information on behalf of the Council in accordance with the Data Protection Act 2018 and General Data Protection Regulation.

2. Targeted Audience and Scope

This policy applies to:

- Employees of Brighton & Hove City Council
- Organisations commissioned by BHCC and their staff
- Service delivery partners and their staff

3. Background

The purpose of this policy is to define the standards and procedures expected of people ("data subjects") when processing personally identifiable information on behalf of the Council in an official capacity.

The General Data Protection Regulation and the Data Protection Act 2018 introduce several changes concerning whether personal data can lawfully be processed. There are also new and strengthened data subject rights, which impose new duties on the Council when collecting and using personal data

Brighton & Hove City Council is committed to protecting the privacy of individuals and handling all personal information in a manner that complies with the General Data Protection Regulation. The Council has established this policy to support that commitment.

4. Definitions

Personal Data – Any data relating to a living person who is directly or indirectly identifiable

Special Category Data – data relating to a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

Data Controller – The organisation which either individually or jointly decides the purposes and methods of data processing.

Data Processor – An organisation which processes data on behalf of the data controller

Processing – Just about anything which can be done with personal data

5. General Principles/ Guidelines

All organisations which handle data about living individuals must comply with the Data Protection legislation, the purpose of which is to protect the rights of the individual (referred to

as data subjects under the Act) when dealing with their personal or sensitive personal information.

It is worth noting that personal data includes opinions expressed about a person or information which sets out an organisation's intentions towards them.

Personal data can only be processed where there is a legal basis for doing so.

Due to its higher level of sensitivity, special category data can only be processed where an additional legal basis for processing (as set out in Article 9 of the General Data Protection Regulation) can be met.

However, data protection is not simply a barrier to using personal information. It provides a framework to ensure that data is shared in the interest of the person whose data it is or where there is an overriding public interest in doing so.

It is not always necessary to obtain the consent of data subjects when processing data. Often the legal basis on which information is held and used by the Council is not consent. However it is necessary to be transparent when collecting somebody's information about the purposes it will be used for and if it will be shared.

The General Data Protection Regulation has introduced the principles of Privacy by Design and Privacy by Default.

When planning to put data into a new system, use it for a new purpose or share I with a new organisation, it is necessary to conduct a Privacy Impact Assessment in order to work out how the risks to personal privacy can best be controlled.

6. The Data Protection Principles

There are six data protection principles:

- Data must be processed fairly, lawfully and in a transparent manner
- It must be processed for specific, explicit and legitimate purposes and not further processed for any purposes which are incompatible with these
- Data must be adequate, relevant and not excessive for the specified purpose
- It must be accurate and where necessary up to date
- Data should be kept in a form where people can be identified from it for no longer than necessary
- There should be appropriate information security to prevent unauthorized processing, or accidental loss or damage to data

The Council is accountable to data subjects for compliance with the above principles and is required to demonstrate that it is compliant.

7. Roles and Responsibilities

The Corporate Management Team ("CMT") is responsible for ensuring that staff operate in accordance with the contents of this policy.

Departmental managers are responsible for the development and propagation of recording procedures which respect the principle of data minimization.

Information Asset Owners are accountable for ensuring that the categories of personal data processed by their service are recorded on their Information Asset Register and that Data Privacy Impact Assessments and Information Sharing Agreements have been put in place where necessary.

The Data Protection team are responsible for implementing this policy and provide advice and investigatory guidance in the event of a Data Protection breach.

All staff are responsible for adhering, reading and understanding this policy.

8. Training Requirements

As a minimum all staff are required to complete Information Governance E-Learning on an annual basis

9. Risks

Brighton & Hove City Council recognises the risks associated with users handling information in order to conduct official Council business.

In the event of a breach action may be taken against the Council (as the Data Controller) and/or the employee responsible for the breach.

Non-compliance with this policy may result in damage or distress to an individual/individuals, financial loss, compromise our ability to provide services to our customers and/or cause damage to the Council's reputation.

The Information Commissioners' Office ('ICO') has the power to issue fines of up to £16,000,000 for breaches of the act. Alternatively they may order the Council to stop processing of personal data where they have cause to believe there is a serious risk to personal privacy.

10. Review of this Policy

This policy will be reviewed annually.

11. Cross References

Acceptable Use Policy
Information Security
Policy Information
Handling Policy
Information Sharing
Policy
Data Quality Policy

12. References

Data Protection Act 2018
ISO 27002: Code of Practice for Information Security
Management ICO Best Practice Guidance
Freedom of Information Act 2000
Regulation of Investigatory Powers Act 2000

13. Policy Control Details

Policy Name	Data Protection Policy
Document Type	User Policy

Version	2.1
Introduction Date	16 July 2011
Effective Date	14 October 2018
Next Review Date:	14 October 2019
Reviewed by:	Information Governance Board
Approved by:	Executive Director of Finance and Resources
Document Author	Data Protection Manager
Document Owner	Senior Information Risk Owner

Please find all Information Governance policies here.