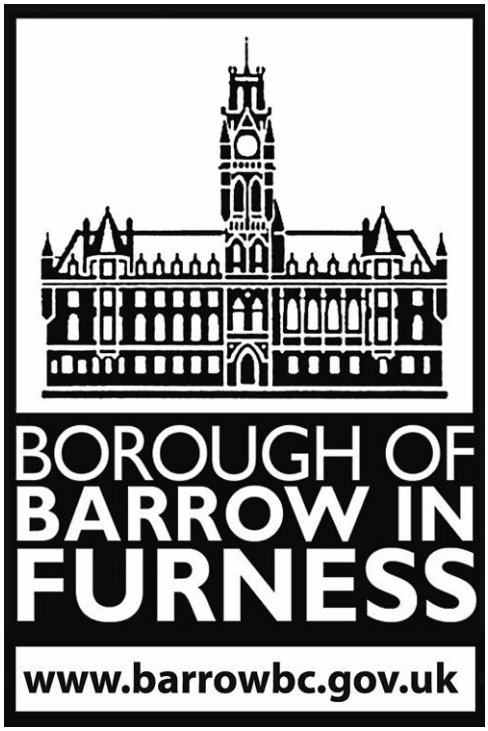

General Data protection Policy

Version Control:	
Document Name:	General Data Protection Regulation Policy
Version:	Version 2.0 Replaces Version 1.0
Author:	Corporate Support Manager
Approved by:	Executive Committee Minor revisions approved by Director of Resources 25 July 2019
Date Approved:	20th March 2018
Reviewed	July 2019.
Review Date	March 2022

Contents

1.0 Introduction

The EU General Data Protection Regulation ("GDPR") (Regulation (EU) 2016/679) replaced the Data Protection Act (DPA) 1998 as the primary instrument for managing data on 25th May 2018.The requirements for processing personal data are similar to the DPA but GDPR sets new standards for data management which require the Council as the Data Controller to have a better understanding of the personal data we hold. We need to ensure that we determine a lawful basis for processing data, document why we are processing it and ensure that the data is not used for other purposes.

We are required to have robust controls in place to ensure that the data we hold is processed securely to ensure it is not unlawfully destroyed, lost, altered or disclosed. If there is a security breach we must have procedures in place to manage and if necessary report it to the Information Commissioners Office.

This policy sets the responsibilities of all employees, managers, councillors and third parties who have access to personal data which is held or processed by or on behalf of the Council.

The definition of personal data is similar to the DPA definition with some additions. The definition of personal data is explained in more detail in the definitions section on page 3 of this document.

2.0 Purpose

The purpose of this General Data Protection Regulation Policy is to ensure that the Council and people working on its behalf, which includes employees, temporary staff, contractors, volunteers, consultants, partners (and their staff) and Members of the Council, understand their obligations under GDPR.

Barrow Borough Council holds and processes personal information about people we provide services for carry out other business with, including:

- Customers
- Residents
- Councillors
- Suppliers
- Contractors
- Employees

People who provide us with their personal data expect us to protect their data and only use it for the lawful purposes we collected it for.

3.0 Scope

All the personal data we hold must be dealt with lawfully and properly. We need to ensure we collect it, store it and process it in a manner that safeguards the privacy of the individuals. The framework for processing of data are defined in the Data Protection Act 2018. The Regulation sets out a framework based on a set of data protection principles.

This policy identifies designated personnel and their responsibilities.

Procedures relating to the collection, processing, storage, retention and disclosure of personal information are referenced in this policy.

Supporting legislation

The statutory legislation below informs the Council's data protection arrangements

The General Data Protection Regulation 2016	This is a framework of responsibilities and rights to strengthen and unify data protection for all individuals.
The Human Rights Act 1998.	Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'.
Crime and Disorder Act 1998	S.115 of the Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act and associated Regulations.

4.0 Definitions

Personal Data
Personal data for GDPR purposes is defined as:

data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Also incudes:

Name
Address
Email Address
Photograph
Bank details
National insurance number
Medical information
Posts on social media sites
Computer IP address

The Information Commissioners Office (ICO) has produced a reference guide and flow chart to help identify personal data and this is available on the ICO website quick guide and a flow chart is attached as appendix 1.

Special category data
GDPR also makes provision for handling special category data (formerly sensitive data). These types of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination and therefore needs more protection. For example, information about an individual's:

Special category data includes

- Race
- Ethnic origin
- Political opinion
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life or

- sexual orientation

We will routinely undertake audits in each department so we can understand the data we hold about individuals and how we process it. We are registered with the Information Commissioners Office registration number Z67771X.

5.0 The Data controller

Barrow-in-Furness Borough Council is the data controller and is accountable for ensuring the data is processed correctly and securely.

6.0 Data processors

Any officer with line management responsibility, this includes supervisors.

All staff, including temporary/agency staff, Elected Members, contractors and volunteers working for The Council**.**

7.0 Information Asset

Data on any media format created, processed and used by the council. Media formats may vary from paper copies (memos, letters, check stock, etc.); electronic files stored on hard drives, USB flash memory devices, CD's, DVD's, back-up tapes etc.; to voice mail. An alternate definition - Information that has value to the extent that it enables an entity to achieve goals and thus is an asset like people, money, and material.

8.0 Data Subject

The data subject is any living individual about whom data is processed.

9.0 Processing

Processing in relation to data (or information) means virtually any use that can be made of the data, from collecting the data, using it, storing it, and destroying it. Any action involving data, should be considered as processing within this definition.

10.0 Manual Data

Manual Data covered by the Data Protection Act 1998 is any non-automated information system (paper files, card index, Rolodex, non-automated microfiche) or 'relevant filing system' referring to data subjects. Filing systems are structured, either by reference or by criteria relating to individuals, in such a way that specific information relating to particular data subjects is readily accessible.

11.0 Data Protection Principles

GDPR requires that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes unless there is a legal requirement for us to do so. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

g) personal data shall not be transferred to a country outside the European Economic Area.

12.0 Lawful basis for processing data

The lawful reasons for processing data are:

1: We have positive, explicit consent from the data subject (consent by default is not permitted e.g. pre-ticked boxes)

2: Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.

3: Processing is necessary for compliance with a legal obligation.

4: Processing is necessary to protect the vital interests of a data subject or another person.

5: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6: Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Please note: basis 6 is not available to processing carried out by public authorities in the performance of our tasks.

13.0 Governance of personal data

Director of Resources

The Director of Resources has overall responsibility for data protection within the Council. The Director of Resources is also designated as the Council's Senior Information Risk Owner (SIRO).

Corporate Support Manager (Data Protection Officer)

The Corporate Support Manager is the Council's designated Data Protection Officer (DPO) the duties of the DPO include:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, awareness- raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO in the UK);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data
- Shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing

All correspondence with the Information Commissioner on Data Protection matters will be dealt with by the Data Protection Officer.

Requests for personal data can be referred to the Data Protection Officer if an officer requires support in determining whether it should be disclosed.

The Data Protection Officer will provide advice in all matters relating to GDPR

Information Sharing Agreements will be signed on behalf of the Council by the Director of Resources or Corporate Support Manager.

Managers

All managers are responsible for ensuring that this policy is communicated and implemented within their area of responsibility. They are responsible for the quality, security and management of personal data in use in their area.

They also need to ensure that their staff are aware of their responsibilities under GDPR. Advice or assistance regarding this policy or GDPR in general is available from the Data Protection Officer.

Managers are responsible for reporting all data protection and information related incidents to the Data Protection Officer, and for ensuring that they are properly investigated according to The Council's incident management procedures.

Elected Members

Elected Members acting for or on behalf of The Council must be aware of their obligations and responsibilities with regards to the collection and processing of personal data under the provisions of the Data Protection Act 1998 and it is the intention of the Council to comply with all aspects and requirements of the Act.

Elected Members have an individual responsibility to keep themselves aware of The Council's policies, including data protection and information security policies.

Data Protection training will be provided for all Elected Members and officers.

Elected Members are expected to co-operate in full with any investigation undertaken by (or on behalf of) The Council into an alleged breach of the regulation.

Elected Members should register with the Information Commissioner's Office and renew their registration annually if they use Information Technology to process personal data e.g. if you use a computer for your constituency work (not work for or on behalf of The Council).

All Staff

All staff have a responsibility to ensure they are aware of their obligations and responsibilities under the Council's GDPR Policy.

All staff should notify their line manager if they feel they do not have sufficient knowledge in regard to GDPR so specific training can be provided.

Staff Members are expected to co-operate in full with any investigation undertaken by (or on behalf of) The Council into an alleged breach of the regulation.

14.0 Auditing

The Corporate Support Department will undertake an annual audit of data management arrangements from a sample of departments and will develop a checklist and templates to support this. The outputs from these audits will be recorded in an auditing plan.

15.0 Managing the data

The Council has adopted a “privacy by design” approach to GDPR. This approach is not a requirement but represents best practice and will make it easier for staff to understand their obligations under GDPR.
A set of protocols setting out the Council’s approach will support this document, which include:

Privacy Notice
Consent Procedure
Data Breach Reporting Procedure

Data asset register

A list of the type of personal data held by each department will be stored on a central asset register held by Corporate Support. Each departmental manager will be responsible for ensuring that their part of the register is maintained.

Under GDPR there is more emphasis on individual’s privacy which includes being transparent about the data we hold and how we will use it.
We have developed a privacy protocol to standardise our approach which provides advice on privacy notices, obtaining consent from data subjects, information sharing, retention periods and the individual’s rights.
We will publish a Privacy Notice and we will be clear about how we collect, store and use individual’s personal data. We will be clear about people’s rights under GDPR.

Managers will undertake a Privacy Impact Assessment before introducing significant changes to data management arrangements or introducing new technologies. These assessments will be reviewed and approved by the DPO.

Consent from data subjects for using their data will require a positive indication that they permit us to use their data for the specific purposes we have informed them we will use it for. We will produce a separate protocol to give clear guidance to managers and staff on how and when we need to obtain the consent of the data subjects.

To perform some Council functions we need to share personal data with third parties. We will be clear about, who we will share it with, what it will be used for and how we will protect their personal data.
We may also share personal data for the prevention or detection of crime including fraud and we need to inform the data subject that their data may be used for this purpose.

A key factor in complying with our lawful basis for processing data is the length of time we retain personal data. The Council’s retention policy will be reviewed on a regular basis to ensure we respect individual’s privacy whilst not compromising the Council’s ability to function.

Under GDPR individuals have enhanced rights regarding the data we hold and how we process it. This means we need to be proactive in informing the customer of how we will process their data and their right to access and change the data we hold about them. A

separate protocol has been developed to help managers to understand their responsibilities in terms of individual's privacy and rights.

The Council and our employees are bound by a legal duty of confidentiality to all data subjects and we have put adequate controls in place.

GDPR applies to all staff (including temporary/agency staff), contractors and volunteers working for the Council.

We will undertake a review of all contractual arrangements which involves third parties processing the Council's personal data. The Data Protection Officer will have responsibility for ensuring that contractual arrangements are compliant with GDPR.

16.0 GDPR Awareness

Training

The Council will develop a training programme which includes maintaining awareness of data protection, confidentiality and security issues for all staff.
This will be provided through:

- Data protection awareness so that staff and councillors understand their responsibilities as part of the Council's induction process.
- External specialist training sessions for managers and staff who have a key role in data protection.
- E-learning modules for all staff.
- Additional training as identified.
- Internal work place training delivered by departmental managers.

Separate training will be provided for Elected Members.