BARNSLEY
Metropolitan Borough Council

Data Protection Policy

Document Control

Organisation	Barnsley Metropolitan Borough Council
Title	Data Protection Policy
Author	ICT Manager
Owner	Senior Information Risk Owner
Commencement Date	25th May, 2018
Applicable to	All Barnsley MBC employees and agency staff, contractors, all elected members, or anyone working on Council premises or on behalf of the Council
Information/ Action	For information and appropriate action to comply with this policy
Review Date	Policy to be reviewed 1 year from approval or when changes are made to legislation or best practice guidance
Review Responsibility	Information Governance Board

Revision History

Date	Version	Author	Comments
March 2018	0.1	ICT Manager	New Policy to meet requirements of data protection legislation
May 2018	1.0	ICT Manager	Approved Policy - Published

Document Distribution

This document will be distributed to the following for review and feedback prior to approval:

Name	Date Issued for Review	Approval Date
Information Governance Board	14/2/18	16/03/18
Senior Management Team	16/3/18	27/03/18
Trade Unions	16/3/18	28/03/18

Policy Governance

The following table identifies who within BMBC is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – The person(s) responsible for developing and introducing the policy
- **Accountable** – The person who has ultimate accountability and authority for the policy
- **Consulted** – The person(s) or groups to be consulted prior to final policy implementation or amendment
- **Informed** – The person(s) or groups to be informed after procedure implementation or amendment.

Responsible	Information Governance Board
Accountable	Andrew Frosdick (SIRO)
Consulted	BMBC Information Governance Board, Senior Management Team, Trade Unions
Informed	All Barnsley MBC employees, contractors, all elected members, or anyone working on Council premises or on behalf of the Council

TABLE OF CONTENTS

1 INTRODUCTION

Barnsley Metropolitan Borough Council (the Council) is committed to compliance with all applicable Data Protection law. This includes the General Data Protection Regulation 2016/279 ('the Regulation'), which became enforceable on 25th May 2018 and the Data Protection Bill 2018 (DPB) which became enforceable prior to 25th May, 2018 (this has not yet gone through all of the stages in Parliament).

The Regulation established some new rights for individuals and strengthened some that currently existed. It also provides for increased accountability and processes to demonstrate compliance. The DPB fills in the gaps in the Regulation and addresses areas in which flexibility and derogations are permitted.

An organisation that handles personal data and makes decisions about its use is known as a data controller. The Council is a data controller and is therefore responsible for ensuring compliance with Data Protection law and the requirements outlined in this policy, failure to comply may expose the Council to complaints, regulatory fines and/or reputational damage.

2 SCOPE

This policy applies to the collection, processing and disposal of all personal and special category data held by the Council, which relates to an identified or identifiable natural person (data subject).

This policy sets out the expected behaviours of all Council workers including all employees agency staff, contractors, all elected members, or anyone working on Council premises or on behalf of the Council who have access to any personal data held by, or on behalf of the Council. The Council will use its best endeavours to ensure that all such parties are fully aware of, and abide by their duties and responsibilities under the Regulation.

Specific roles and responsibilities are outlined in Appendix A.

3 DEFINITIONS

A full list of definitions are detailed at Appendix C.

4 POLICY

4.1 Data Protection

The data protection principles set out the main responsibilities of a data controller. These principles are legally enforceable.

- Principle 1: lawfulness, fairness and transparency

This means that the Council will tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject

(fairness), and it must be processed for one of the purposes specified in the legislation (lawfulness).

- Principle 2: Purpose Limitation

This means that the Council will specify what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

- Principle 3: Data Minimisation

This means that the Council will not store any personal information beyond what is strictly required.

- Principle 4: Accuracy

This means that the Council will have in place processes for identifying and addressing out-of-date, incorrect and redundant personal information.

- Principle 5: Storage Limitation

This means that the Council will, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

- Principle 6: Integrity and Confidentiality

This means that the Council will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal information is maintained at all times.

- Principle 7: Accountability

This means that the Council will demonstrate that the six Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

4.2 DATA COLLECTION

4.2.1 Consent

The Regulation has strengthened the requirement for getting consent from someone to hold their data. Previously consent was defined as any freely given specific and informed indication of their wishes

The Regulation additionally that consent should be given by a positive, unambiguous, affirmative action. The Council will capture and retain consent, together with the version of the privacy information that accompanied the consent. Data subjects should clearly understand why their information is needed, who it will be shared with and the possible consequences of them agreeing or refusing the proposed use of the data

If the legal basis for processing data is based on consent the Council must respect the individual's right to withdraw consent at any time and in a way that is easy. Refer to section 4.5 detailing individuals rights.

4.2.2 Data subject notification

The Council will, except where there are lawful and compelling reasons not to do so, provide data subjects with information as to the purpose of the processing of their personal data.

The Council is committed to transparency over how it will use personal data. The Council will ensure that all information supplied regarding the processing of personal data is concise, clear, intelligible easily accessible, written in plain language, and is free of charge. The Council has published a Privacy Notice which can be accessed here (Link to Council's privacy notice)

4.3 DATA USE

4.3.1 Data processing

The Council will only process personal data in accordance with all applicable laws and contractual obligations. The Council will not process personal data unless at least one of the legal bases' for processing are met (outlined in Appendix B).

4.3.2 Special categories of data

The Council will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the legal bases' for processing are met outlined in Appendix B.

4.3.3 Children's data

Where services are offered directly to a person under 16 years of age the Council will ensure that the privacy notice is written in language that a child can be expected to understand. If online services are offered to under 16's, the Council will obtain consent from a parent or guardian to process the child's data. Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

4.3.4 Data quality

The Council will always use its best endeavours to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject.

The measures adopted by the Council to ensure data quality include:

- Correcting personal data in a timely manner that is discovered to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.

- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.

- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.

4.3.5 Profiling and Automated Decision Making

The Council will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law.

The Council will advise Individuals where this takes place and that they have the right not to be subject to a decision when it is based on automated processing. The Council will ensure that individuals are able to obtain human intervention; express their point of view; and obtain an explanation of the decision and challenge it.

4.4 PROTECTION OF DATA

4.4.1 Data Storage and Security

The Council has deployed a range of physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing.

The minimum set of security measures to be adopted by the Council is provided in the Council's Information Security and Computer Usage Policy (link).

4.4.2 Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them will go through an approval process before continuing. A data protection impact assessment will be conducted which will allow the Council to assess the impact of, the new or altered processing operations, on the protection of Personal Data. Detailed guidance can be found in the Data Protection Impact Assessment Policy. (link)

4.5 DATA SUBJECT REQUESTS AND ADMINISTRATION OF INDIVIDUAL RIGHTS

4.5.1 Data Subject Requests

Where an individual wishes obtain information regarding the personal data the council holds about them, they can make a data subject request. The Council will deal with data subject requests asset out in the Council's privacy notice (link). Data Subjects are entitled to obtain, based upon a request made in writing to the Council and upon successful verification of their identity, information about their own personal data .

The Council will not charge for data requests but will charge a 'reasonable fee' if requests for information is manifestly unfounded or excessive.

Data requests will be responded to without undue delay and at least within one month of the request. This may be extended to two months if the information is complex the data subject will be informed of this within one month of the request.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information will be redacted or withheld as may be necessary or appropriate to protect that person's rights. Where personal data have not been obtained from the data subject the Council will provide the data subject with information as to the identity and contact details of the Data Controller.

Detailed guidance for staff making and dealing with requests from data subjects can be found in the Council's Information Request Procedures' (link) document. Detailed guidance for data subjects on how to make a request can be found on the Council's external website (link).

4.5.2 Administration of Individuals rights

Data Subjects have a number of rights that they can exercise with regards the processing of their personal information. The Council will investigate and respond without undue delay and at least within one month of the notification, where appropriate with supporting action taken. Individual's rights are set out in the Council's privacy notice (Link).

The Council has also established processes in respect of a number of data subject rights:

1. Right to be informed: the Council must provide 'fair processing information'.

2. Right to access: confirmation that their data is being processed; access to their personal data; and other supplementary information.

3. Right to rectification: people can have corrected incorrect information.

4. Right to erasure: that is to be forgotten.

5. Right to restriction of processing: the Council can store but not process the data.

6. Right to portability: to take and reuse their personal data across a range of services.

7. Right to human intervention in automated decision making processing: to cease processing unless the Council can demonstrate that it either has compelling grounds for continuing, or that the processing is necessary in connection with its legal rights.

8. Right to automated decision making: people can object if a human is not in the loop on a decision about them.

4.6 LAW ENFORCEMENT AND DISCLOSURES

Where the Council controls or processes personal data for any law enforcement purpose, for example, the investigation or prosecution of an offence, this is outside the scope of the Regulation. The rights and obligations of data controllers, processors and subjects where data is held for law enforcement purposes are to be set out in Part 3 of the Data Protection Act 2018 and will be subject to a separate policy.

In broad terms the law enforcement provisions prescribe that in certain circumstances, it is permitted for personal data be shared without the knowledge or consent of a data subject if this is necessary for the purposes of:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

4.7 DATA TRANSFERS

The Council may transfer personal data to third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Personal data will only be transferred outside of the EU in compliance with the conditions for transfer set out in the Regulation.

Where the third party is deemed to be a data processor, the Council will enter into an adequate agreement. The agreement will require the data processor to protect the personal data from further disclosure and to only process it in compliance with the Council's instructions.

4.8 DATA PROTECTION TRAINING

All Council employees, agency staff, volunteers, contractors, elected members, or anyone working on Council premises or on behalf of the Council who have access to any personal data held by, or on behalf of the Council will be subject to mandatory staff induction and thereafter annual training so that they will understand their responsibilities under this policy. Failure to complete within the approved allocated timeframe and attaining the accepted pass rate will result in individuals having their network access revoked until this has been achieved. In addition, the Council will provide regular updates on information governance and information security developments.

4.9 COMPLIANCE

The Council has appointed a Data Protection Officer (DPO) will undertake the minimum prescribed tasks as follows:

- inform and advise the Council at the highest level about all data protection matters and ensure that all of its employees understand their obligations to comply with the Regulation and other data protection laws
- monitor compliance with the Regulation and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits and
- be a named point of contact for the Information Commissioner's Office and for individuals whose data is processed

The DPO for the Council can be contacted via email at DPO@barnsley.gov.uk. The specific role and responsibilities of the DPO are outlined in Appendix D.

4.10 COMPLAINTS HANDLING

Data subjects with a complaint about the processing of their personal data should contact the Customer Feedback and Improvement Team (CF&IT). (link to external website)

Barnsley MBC

Corporate Services

C/O Corporate Mail Room

PO Box 634

Barnsley

S70 9GG

Email: informationrequests@barnsley.gov.uk

An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case.

If the issue cannot be resolved then the Data Subject may, at their option, seek redress through contacting the Information Commissioner's Office directly at:

Customer Services Team

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

SK9 5AF

4.11 BREACH REPORTING

A personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

The Council has a duty to report certain types of data breach to the relevant supervisory authority (Information Commissioner's Office), and in some cases to the individuals affected.

Following initial assessment the Council will report all breaches classified within the 'notifiable criteria' to the Information Commissioner's Office within 72 hours of becoming aware of it. If the breach is sufficiently serious to warrant notification to the public, the Council will do so without undue delay.

Any individual who suspects that a personal data breach has occurred must immediately notify the Information Governance Team and follow the guidance set out in the Information Security Incident Reporting Policy (link)

A failure to notify a breach when required to do so can result in a fine of up to 10 million Euros.

The penalty for committing a breach can be up to 20 million Euros!

4.12 POLICY MAINTENANCE AND MONITORING

The Council's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

To confirm that an adequate level of compliance that is being achieved in relation to this policy an annual data protection compliance audit will be carried out. In addition, the

Information Governance Board and Audit Committee will receive regular assurance reports on the effectiveness of data protection related activities.

The policy will be reviewed on an annual basis, or as and when legislation or best practice guidelines change.

4.13 RELATED DOCUMENTS

Information Security and Computer Usage Policy

Information Security Incident Reporting Policy

Data Protection Impact Assessments Policy

Records Management Policy

Guidance Documents – to outline (Claire Dobby's procedures)

Appendix A – ROLES AND RESPONSIBILITIES

Role	Responsibility
Service Director (Customer Information and Digital)	Accountable for ensuring that all systems, services and equipment used for processing, storing and archiving data meet acceptable security standards Ensure that regular health checks and scans are performed to ensure hardware and software are functioning properly Perform thorough due diligence on any third party services the Council are considering to store, process or archive data eg Cloud Computing Services
Caldicott Guardian	Caldicott Guardian is responsible for the safeguarding of information processed for social care work and will oversee all procedures for protecting the confidentiality of service user information and enabling the appropriate information sharing. The Caldicott Guardian will ensure that compliance with this policy is achieved and will work proactively (supported by nominated officers) to ensure that personal data processed for social care is appropriately safeguarded to meet the requirements of data protection law and other information rights legislation
Data Protection Officer	Responsible for devising and implementing and thereafter for the operation and maintenance of the whole of the Council's strategic and operational response to the requirements of the new data protection regime and to personally provide to the Council's highest level of management autonomous and independent oversight and assessment of corporate compliance, recommending and implementing changes necessary, including the development of strategies for long term future implementation. To inform and advise the Council and its employees about their obligations to comply with the GDPR and other data protection laws. To advise on data protection impact assessments; train staff and conduct internal audits. To be the first point of contact for the Information Commissioner's Office and for individuals whose data is processed (employees, customers etc)
Executive Directors, Service Directors and Heads of Service	Are accountable for data protection matters in their own business units of work including: • development, implementation and review of directorate procedures that support this policy.

	• ensuring compliance with the policies and standards set out in this policy and ensure staff are aware of their responsibilities. • ensure that staff are trained and experienced when accessing personal information • ensure that new information systems, processes or policies in their business units are designed to comply with this policy (data protection impact assessment). • notifying the Service Director of any potential new customer information and digital systems in their area of work that process personal data
All Council employees, agency staff, other workers, volunteers, contractors, elected members, or anyone working on Council premises or on behalf of the Council who have access to any personal data held by, or on behalf of the Council	Will have immediate responsibility to; • comply with the requirements of this policy; • proactively alert management to suspected poor data protection practices and data breaches
Information Governance Board	Provide a strategic lead in creating and sustaining an information culture within the Council and with its partners. To ensure that there is clear direction and visible management support for information governance initiatives. To ensure decisions made at IG Board are disseminated down throughout their respective Business Units and to promote information governance and information security practices.
Customer Services Feedback and Improvement Team	Provide data subjects with a triage service to process any individuals' rights principles and ensure the Business Units comply with the timeliness of these requests and escalate to the DPO where there is non-compliance. This includes: 1. Right to be informed 2. Right to Access 3. Right to rectification 4. Right to erasure 5. Right to restriction of processing 6. Right to portability 7. Right to object 8. Right to decision making
Senior Information Risk Owner (SIRO)	The SIRO role is to lead and champion the Council's information risk policy, and provide advice and assurance to the Information

	Governance Board regarding information and security risk
Information Governance Team	Responsibility for developing Policy to meet Data Protection legislation. To ensure Policy review and revision arrangements are in place. To support the role of the Data Protection Officer Devise data protection related training and awareness for staff Facilitate and provide advice and guidance on IG related issues for example, information security data breaches, DPIA's, privacy notices etc
Audit Committee	The overall function of the Audit Committee is to improve focus in the council on the issues arising from risk management, internal control and reporting. The Audit Committee will review reports relating to data protection and the main issues arising and will seek assurance that action has been taken

Appendix B

Lawful processing

For processing to be lawful under Data Protection legislation and defined in the GDPR, the Council will identify and document a legal basis before they can process personal data. These are referred to as the "conditions for processing".

This becomes more of an issue under the GDPR because your legal basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data erased.

The tables below set out the legal bases available for processing personal data and special categories of data.

Lawfulness of processing conditions – personal data

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – 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(1)(f) – Necessary for the purposes of legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

Conditions for special categories of data – sensitive data

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Appendix C - Definitions

Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Protection	The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.
Data Processors	A natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.
Data Subject	The Identified or Identifiable Living Natural Person to which the data refers.
Employee	An individual who works part-time or full-time for the Council under a contract of employment, Includes temporary employees.
Identifiable Natural Person	Any living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data	Is categorised as personal information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise Processed.
Profiling	Any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an Identifiable living person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Process, Processed, Processing	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include 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.
Special Categories of Data	Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Party	An external individual or organisation with which the Council conducts business and is also authorised to, under the direct authority of the Council process personal data.

Appendix D – Data Protection Officer – Roles and Responsibilities

The Council has an obligation as a public authority, which processes personal and special categories of data, under Data Protection Legislation to appoint a Data Protection Officer.

To fulfil their obligations of this role for the Council the appointed Data Protection Officer will:

- Be fundamental in assisting the Council demonstrate its accountability for the proper management of personal and special data
- Have involvement in a timely manner in all issues which relate to the protection of personal and special data that we hold about individuals. This includes all data breaches reported and investigated by the Council;
- Report and have unfettered direct access to senior management in the Council on data protection matters. The independent and impartial advice and recommendations made by the DPO with regards data protection matters will be taken into consideration by senior management
- Be consulted and advise on changes to existing and the implementation of new systems that are used for the purpose of processing personal and or special data;
- Be provided with adequate support from the Council in terms of resources, infrastructure and staff to fulfil the requirements of the role;
- Ensure there is effective monitoring in place and compliance with Data Protection laws, including the management if internal data protection activities, ensuring data processing staff are trained and commission and conduct appropriate audits;
- Have up to date knowledge of the Council's obligations regarding data protection legislation and hold a relevant qualification. This will be supported with continuous training;
- Work alongside and cooperate with the Council's supervisory authority (the Information Commissioner Officer) and serve as the contact point for the supervisory authority on issues relating to the processing of personal data;
- Be available for inquiries from data subjects and staff members on issues relating to data protection practices and the failure to comply with data protection principles; and
- Be bound by confidentiality concerning the performance of their task.

Contact details for the Councils Data Protection Officer: DPO@barnsley.gov.uk