Blaby District Council **Policy**

Data Protection Policy (Incorporating the Requirements of the GDPR)

Original Publish Date	25/05/2018	**Review Frequency**	Every 2 years	**Current Version Publish Date**	25/05/2018
Approved By*	Council	**Approval Date***	22/05/2018	**Version Number**	001
Author Job Title	Data Protection Officer	**Service Area**	Information Governance	**Document Register Reference**	A 902

*Approved by and 'approval date' are in relation to the most recent version.

Review History			
Version*	Reviewed By (Job Title)	Review Completion Date	Brief Description of Changes (add 'no changes required' if applicable)
001	Principal Information Governance Officer	7 June 2024	No changes required.

*Version number remains the same if no significant changes are made upon review.

Document Definition / Approval & Review

Defining the document type and how it is approved and reviewed

Blaby District Council policies **'outline a set of rules or principles that govern how the council (or services within the council) will operate'.**

Key published documents are approved for publication in line with the approval matrix illustrated in the Key Published Document Procedure.

Unless agreed by exception, key published documents must be reviewed at least **every 3 years** from the date of approval.

Significant updates/changes must also seek reapproval in line with the approval matrix.

Scope

To what and to whom this policy applies

The purpose of this policy is to ensure that all elected members, employees and agents acting for and on behalf of the council are aware of their obligations and responsibilities with regard to the collection and processing of personal data under the provisions of the Data Protection legislation and that it is the intention of the council to comply with all aspects and requirements of the legislation.

Terms & Definitions

Definition of any acronyms, jargon, or terms that might have multiple meanings.

Term	Definition

Policy Sections

Section 1 Introduction

The purpose and reason for this policy is to support services with adherence to legislative requirements where the Council collects and processes personal information. The Council is fully committed to complying with the Data Protection legislation and is registered as a Data Controller with the Information Commissioners Office.

It is the responsibility of every employee and elected member of Blaby District Council to comply with the obligations under the legislation and this policy. In addition, Blaby District Council requires its partners and contractors who act on its behalf to comply with the legislation when providing services to and on behalf of the council.

Section 2 – Data Protection Legislation

The legislation relevant to this policy are set out below.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive).

- Data Protection Act 2018.
- Protection of Freedoms Act 2012.
- Human Rights Act 1998.

Section 3 – Definitions

All the terms used within this policy have the meaning assigned to them within General Data Protection Regulation.

CCTV includes Automatic Number Plate Recognition (“ANPR”) Licence Plate Recognition Cameras (“LPR”), body worn cameras, webcams, covert installations and any other system capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals

Section 4 – Data Protection Principles

Article 5(2) of the General Data Protection Regulation provides that the Data Controller is responsible for compliance with the following principles.

- Personal data is processed lawfully, fairly and in a transparent manner in relation to individuals.

- Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 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.

- The processing and retention of personal data is adequate, relevant and limited to what is necessary in relation to the purposes for it is used.

- Personal data is accurate and where necessary is kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer period insofar as the personal data will be proceed 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.

- 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.

Section 5 – The Rights of Individuals

The 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.

Section 6 – Accountability

The council is committed to complying with the provisions of the Data Protection legislation and the six data protection principles by ensuring the following.

- The Council keeps and maintains the records required to comply with its accountability obligations, including records of processing activities as required.

- A Data Protection Officer (DPO) is appointed and that suitable cover arrangements are in place at all times.

- The Council, the Electoral Registration Officer, its Elected Members and any other officer which may be required to be, is registered with the Information Commissioner's Office as appropriate.

- All elected members, employees, and third parties acting on behalf of the Council are aware of their responsibilities and the consequences of non-compliance with this policy or breaches of the Data Protection legislation through the provision of training and awareness programs.

- There are technical and organisational measures in place to always ensure the security of personal information.

- There are appropriate procedures in place for acknowledging and handling subject access requests and other individual's rights to enable individuals to exercise their rights without undue delay.

- Data Protection, privacy by design and the use of Data Protection Impact Assessments where changes to policy and procedure could affect individuals.

Section 7 – Responsibility

All elected members, employees and agents acting for the council are responsible for ensuring that personal data that they collect, and process is done so in accordance with the Data Protection legislation and this policy.

All Managers are responsible for identifying training needs within their areas and ensure that this policy has been read and understood by members of their teams.

Any staff who are using their own personal devices for the purposes of Teams Meetings must ensure that their device is suitably encrypted to protect any information transferred and potentially stored on their device via the Microsoft Teams software. If you have used your personal device for a Teams meeting and then lose your device, please refer to the breach reporting procedure below.

Section 8 – Breaches

All individuals are responsible for reporting any data breach to the Data Protection Officer, who will determine whether the breach should be reportable to the Information Commissioners Office and take immediate actions to address the breach.

Advice & Guidance

If any elected member, employee, or agent of the council requires advice or guidance on the provisions of this policy, relevant legislation or supporting guidance then please contact the Information Governance team via GDPR@blaby.gov.uk.