LICENSING, AUDIT & GENERAL PURPOSES COMMITTEE
Corporate Manager- Legal Services

25th November 2019 **REPORT NO. LSIG 19/11**

DATA PROTECTION POLICY and DATA PROTECTION OFFICER APPOINTMENT

SUMMARY:
A Data Protection Policy has been developed to set out how RBC complies with its duties under the EU General Data Protection Regulations (GDPR) and the UK Data Protection Act 2018 (DPA 2018) together Data Protection Legislation.

RECOMMENDATION:
Members are requested to:

- Approve the Council's Data Protection policy, and
- Delegate authority to the Corporate Manager – Legal Services to keep the Policy under review and update as required

1 Introduction

1.1 It is essential that we have an up to date Data Protection Policy as part of the accountability to the Information Commissioner's Office (ICO) in demonstrating our approach to Data Protection. The ICO is the Data Protection regulator in the UK.

2. Data Protection Policy

2.1 The Data Protection Policy forms part of the Information Governance Framework which is being rolled out to all teams setting in place the processes and procedures to securely access information held by the organisation when and where required. The purpose of the Data Protection Policy is to explain the Council's approach to staff, Members and customers ensuring that we comply with the Data Protection Legislation when we collect, process and store the personal data that we need in order to carry out our business. The Policy explains in clear terms how the GDPR applies to employees, Members and contractors and what their obligations are. Article 24 of the GDPR specifies that organisations create a policy in order to "demonstrate that [data] processing is performed in accordance with this Regulation".

2.2 The Policy will be kept under review annually.

Owner / Head of Service:
Catriona Herbert**,** Legal Services and Deputy Monitoring Officer
01252 398616
Catriona Herbert@rushmoor.gov.uk

AUTHOR: Bridgette Burrows - Information Governance
bridgette.burrows@rushmoor.gov.uk

RUSHMOOR BOROUGH COUNCIL

Data Protection Policy

N.B. Staff are discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

1. Introduction

1.1 This document sets out Rushmoor Borough Council's ('the Council') Data Protection Policy and how it complies with the Council's duties under the EU General Data Protection Regulations (GDPR) and the UK Data Protection Act 2018 (which in combination constitute 'the legislation').

1.2 The legislation regulates the way in which personal data about individuals, whether held digitally or in a manual filing system, is subjected to any processing operation, including collection, storage, use, disclosure and destruction.

1.3 The Council needs to process personal data and sometimes sensitive personal data about people with whom it deals in order to carry out its statutory duties, perform its functions and to comply with terms of contracts it has entered. This includes information on current, past and prospective service users, employees, suppliers, clients, customers, and others with whom it communicates. It may include all persons who live, work or visit the Borough and many others who do not.

1.4 The Council regards the lawful and correct treatment of personal information as critical to the success and effectiveness of its operations, and to maintaining the confidence of those it serves. It is essential that it respects the rights of all persons whose personal information it holds, that it treats personal information lawfully and correctly in accordance with the legislation and that it can show that this is the case.

1.5 Failure to comply with the legislation infringes the rights of individuals and may place them at risk of loss or harm. It also exposes the Council to challenge, legal claims and substantial financial penalty.

1.6 This policy applies to all staff and elected Members and the Council expects all its staff and elected Members to comply fully with this policy and the principles laid down in the legislation (set out in Section 3 below). Elected Members should adhere to the policy to ensure compliance with the Members' Code of Conduct and the Council's obligations in relation to confidentiality.

1.7 Third parties such as partners, public and private organisations or contractors with whom the Council shares personal data or who hold data on the Council's behalf will be expected to enter into and adhere to formal agreements or contractual obligations with the Council incorporating the principles of this policy and the requirements of the legislation. Such agreements or contracts must define the purposes for which personal data is supplied to or held by the other party and require contractors to have in place appropriate organisational and technical measures to protect the data and processes to enable the exercise of the rights of individuals.

2. Definitions

2.1 Definitions used in the GDPR and in this policy are as follows:

2.1.1 '**Personal data**' is any information relating to an identified or identifiable natural person, either through their name or another identifier such as an identification number.

2.1.2 '**Processing**' refers to any operation performed on personal data, whether by electronic or automated means, such as collection, use, storage, disclosure or destruction.

2.1.3 '**Data subject**' is the term used to describe any given person when identified in relation to their personal data.

2.1.4 '**Data controller**' is the label for organisations which decide how and why personal data is used, while '**data processors**' is a label for organisations responsible for processing personal data on behalf of a controller. Woking Borough Council is a data controller, while its suppliers are data processors.

2.1.5 '**Special categories**' of personal data encompasses ethnicity and data concerning health, among other categories. To process these, there are extra requirements. Similar requirements exist in the GDPR for processing data on criminal convictions or offences.

3. Data protection principles

3.1 The Council will comply with the principles included in the legislation, ensuring that personal data is:

3.1.1 Processed lawfully, fairly and in a transparent manner;

3.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;

3.1.3 Adequate, relevant and limited to what is necessary in relation to those purposes;

3.1.4 Accurate and, where necessary, kept up to date;

3.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary to fulfil the purposes for which the personal data is processed;

3.1.6 Processed in a manner that ensures appropriate security of the personal data;

3.1.7 Processed in accordance with the rights of data subjects.

4. General requirements

4.1 If follows from the principles of the legislation that, in practice:

4.1.1 Personal data should only be processed when an appropriate lawful basis in the legislation can be identified;

4.1.2 Personal data should only be accessed by those who need to for work purposes;

4.1.3 Personal data should not be divulged or discussed except when performing normal work duties;

4.1.4 Personal data must always be kept safe and secure, including at the office, public areas, home or in transit;

4.1.5 Personal data should be regularly reviewed and updated; and

4.1.6 Queries about data protection, internal and external to the Council must be dealt with effectively and promptly.

5. Responsibilities of officers and elected Members

5.1 The Council is a Data Controller under the legislation and must comply with the principles laid down in the legislation and be able to demonstrate compliance with them.

5.2 The Data Protection Officer (Corporate Legal Manager) shall be accountable for the implementation and effectiveness of this policy. The Data Protection Officer shall also have specific operational responsibility for data protection matters corporately.

5.3 All Corporate Leadership Team members are responsible for implementing safe and sound data protection procedures within their areas of responsibility. Corporate Leadership Team members should have regard to this policy and any accompanying guidance issued by the Data Protection Officer from time to time, when formulating procedures which make use of personal data.

6. Data security

Staff should refer to the separate (AUP) Information Security Policy for details on information security.

6.1 All staff are responsible for ensuring that personal data which they use, or process is kept securely and is not disclosed to any unauthorised person or organisation. Access to personal data should only be given to those who have and can show a need for access to the data for the purpose of their duties.

6.2 Personal data should not be left where it can be accessed by persons not authorised to see it or have access to it by reference to this policy and the principles in the legislation.

6.3 Personal data that is no longer required must be destroyed appropriately, for example, by shredding or, in the case of computer records, secure deletion. Personal data must be destroyed in accordance with the Council's retention schedule.

6.4 Staff and elected Members who work from home must have regard to the need to ensure compliance with this policy. The security and proper processing of data outside offices and usual places of work and whilst travelling must be ensured.

6.5 The Data Protection Officer shall ensure that personal data breaches are investigated and, where the breach is likely posing a risk to the rights and freedoms of individuals, reported to the Information Commissioner's Office in line the requirements of the legislation.

7. Information sharing

7.1 Personal data may need to be shared with third parties in order to deliver services or perform our duties. The Council will only share personal data when a lawful basis from the legislation can justify that sharing, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so.

7.2 Disclosure within the Council either to staff or elected Members will be on a need to know basis or to enable the most effective discharge of their responsibilities. Such disclosure may only be carried out when a lawful basis from the legislation can justify that disclosure. It will be carried out in accordance with the principles laid down in the legislation.

7.3 Data Sharing Agreements should be concluded when setting up on-going or routine information sharing arrangements with third parties. However, they are not needed when information is shared in one-off circumstances, but a record of the decision and the reasons for sharing information should be kept. All Data Sharing Agreements must be signed off by the Data Protection Officer, who will keep a register of all Data Sharing Agreements.

8. Data Protection Impact Assessments

8.1 As required by the legislation, Data Protection Impact Assessments ('DPIAs') will be completed in instances when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals.

Such instances may include, but are not limited to:

8.1.1 Introduction of new technologies;

8.1.2 Systematic and extensive processing activities;

8.1.3 Large scale processing of special categories of data or personal data relating to criminal convictions or offences;

8.1.4 Large scale, systematic monitoring of public areas, such as CCTV; and

8.1.5 Before entering a data sharing agreement.

9. The rights of data subjects

9.1 Subject to the provisions of the legislation, Members, staff and members of the public have the following 'information rights' in relation to their personal data:

9.1.1 to be informed about how and why their personal data is processed;

9.1.2 to access their data;

9.1.3 to rectification of their data;

9.1.4 to erasure of their data;

9.1.5 to restrict processing of their data;

9.1.6 to data portability;

9.1.7 to object to processing of their data; and

9.1.8 not to be subject to fully-automated decision-making including profiling.

9.2 The Data Protection Officer will ensure appropriate processes are in place to ensure the Council enables the exercise of these rights, according to the provisions of the legislation.

9.3 Any information rights requests are processed by the Data Protection Officer. Individuals will be expected to submit requests in writing and provide any necessary proof of identification as part of the request.

9.4 The Council aims to respond promptly to these information rights requests and, in any event, within the statutory time limit (normally 30 days). Requests will be managed and tracked by the Data Protection Officer.

10. Complaints

10.1 Anyone who believes that the Council has broken the law can make a complaint. Examples of this are when they think their information has not been obtained fairly, it has not been handled securely or they have asked for a copy of their information and they are not satisfied with the Council's response.

10.2 Complaints regarding the processing of personal data should be made to the Data Protection Officer.

11. Training

11.1 Data protection training is important so that all staff and elected Members understand their responsibilities. Legal advice and guidance on data protection matters are available to all staff and elected Members. Core guidance, practice, procedures and policies shall be held on the Council's intranet. The Data Protection Officer shall ensure that training resources are up to date and promote and ensure the take up of training and advice by staff.

12. Guidance notes

12.1 The Data Protection Officer shall, where appropriate to do so, be responsible for issuing guidance notes explaining the practices necessary to ensure compliance with this policy. These guidance notes shall, when issued, be published on the Council's Intranet.

13. Policy review

13.1 The Data Protection Officer has responsibility for co-ordinating the maintenance and review of this policy.

13.2 Reviews will consider changes in legislation and best practice. The Data Protection Officer is authorised to amend this policy following a review.