Rushcliffe Borough Council Constitution

Part 5

CODES AND PROTOCOLS

INFORMATION SHARING / UK GDPR & DPA 2018

1. Introduction

1.1. The nature of the relationship between the Council and Councillors means that personal data will be shared between both parties. These codes and protocols set out rules and responsibilities to ensure the Council and Councillors meet their obligations to the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA).

1.2. All Councillors are designated 'Data Controllers' and have a responsibility to ensure all safeguarding is in place to secure and protect all personal data as governed by the UK GDPR and DPA 2018.

1.2.1. Data Controller – Article 24 of UK GDPR means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.

1.2.2. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

1.2.3. Where proportionate in relation to processing activities, the measures referred to in section 1.2.2 shall include the implementation of appropriate data protection policies by the controller.

1.3. All Councillors must complete their Information Management and Governance eLearning course. This is to ensure you kept up to date with your responsibilities outlined in this section.

2. Principles relating to processing of personal data

2.1. The UK GDPR sets out seven key principles that all Councillors must following when handling personal data:

(a) Lawfulness, fairness and transparency
(b) Purpose limitation
(c) Data minimisation
(d) Accuracy
(e) Storage limitation
(f) Integrity and confidentiality (security)
(g) Accountability

2.2. Here are definitions for each of these principles.

2.2.1. Personal data shall be:

(a) processed **lawfully**, **fairly** and in a **transparent** manner in relation to the Individuals ('lawfulness, fairness and transparency');

(b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) **adequate**, **relevant** and **limited** to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) **accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of Individuals for **no longer than is necessary** for the purposes for which the personal data are 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Individuals ('storage limitation');

(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 ('integrity and confidentiality').

2.2.2. The controller shall be responsible for, and be able to demonstrate compliance with, section 2.2.1 ('**accountability**').

3. Information to be shared

The information that may be shared between the Council and Councillors are shown under **'What information is being shared'** in Annex 1.

4. Legal Basis for sharing

4.1. All Councillors must take care when processing personal data that a legal basis exists for doing so. In most scenarios, all Councillors will be processing personal data with Consent under Article 6(1)(a) or processing personal data for the purposes of carrying out a public task under Section 8 DPA 2018 and Article 6(1)(e) UK GDPR.

4.1.1 **Article 6(1)(a)** the Individuals has given consent to the processing of his or her personal data for one or more specific purposes. Consent must be recorded;

4.1.2 **Article 6(1)(e)** gives you a lawful basis for processing where 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.

4.1.3 **Act Section 8** a task carried out in the public interest, or the exercise of official authority includes processing that is necessary for the:

(a) administration of justice;
(b) exercise of a function of either House of Parliament;
(c) exercise of a function conferred on a person by an enactment or rule of law;
(d) exercise of a function of the Crown, a Minister of the Crown or a government department; or
(e) an activity that supports or promotes democratic engagement

4.2. To the extent that information being shared with the Council includes any Personal Data, Councillors shall ensure that the Shared Information is processed in accordance with the Data Protection Legislation.

5. Access to data and individuals' rights

5.1. All Councillors must have process and procedures in place to allow Individuals to exercise their individual rights.

5.1.1. The Right to be **Informed** - Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. All Councillors must provide their own Privacy Notice, explaining purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.

5.1.2. The Right of **Access** - Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'. Individuals can make SARs verbally or in writing, including via social media. You should respond without delay and within one month of receipt of the request. All responses must be disclosed securely, and you should provide the information in an accessible, concise and intelligible format.

5.1.3. The Right to **Rectification** - Individuals have the right for inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing and you have one calendar month to respond.

5.1.4. The Right to **Erasure** (right to be forgotten) – Individuals have the right to have their personal data erased however, this right is not absolute and only applies in certain circumstances.

(a) The personal data is no longer required for the purposes for which they were collected or otherwise processed.
(b) Consent is withdrawn on which the processing is based and there are no legal grounds for the processing.
(c) The individual objects to the processing and there are no overriding legitimate grounds for the processing or for direct marketing purposes.
(d) The personal data has been unlawfully processed.
(e) The personal data must be erased for compliance with a legal obligation.
(f) The personal data have been collected in relation to the offer of information society services.

An individual can make a request for erasure verbally or in writing and you have one calendar month to respond.

5.1.5. The Right to **Restrict Processing** - Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing and you have one calendar month to respond to a request

5.1.6. The Right to **Data Portability** – Individuals shall have the right to receive the personal data concerning him or her, which he or she has provided you, in a structured, commonly used and machine-readable format.

5.1.7. The Right to **Object** - Individuals shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. Councillors shall no longer process the personal data unless you can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Individuals or for the establishment, exercise or defence of legal claims. How the Individuals makes such objections shall be detailed in your Privacy Notice.

5.1.8. Rights in relation to **automated decision making** and **profiling** - Individuals have the right to object to automated decision making or profiling. Unless there are grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims, you must stop processing straightaway.

5.2. All Councillors must notify the Council without due delay of any request by an individual for rectification or erasure of Shared Information or restriction of processing carried out in respect of the Shared Information.

5.3. All Councillors will respond to any notice from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.

6. Privacy Notice

6.1. When processing personal data, you must tell individuals what you are doing with it. They have the right to know why you need it, what you'll do with it and who you're going to share it with. You should provide this information in a clear, open and honest way. This is achieved by creating a document called a Privacy Notice.

6.2. All Councillors must have their own Privacy Notice to comply with UK GDPR Article 5 Principle (a) Lawfulness, fairness and transparency. The Councill will provide a template for you to populate and make appropriate for your use. Your Privacy Notice will be published on the main Rushcliffe website with your profile information.

7. Data Breaches

7.1. Councillors must report misuse, loss, destruction, damage or unauthorised access, suspected or otherwise, of information to the Council without due delay.

7.2. The Council must be notified without due delay of any breach of confidentiality or incident involving a risk or breach of the security of personal information.

7.3. Councillors are liable for any losses or liabilities incurred due to their own actions as a result of a breach under the UK GDPR and DPA 2018.

7.4. In the event of any personal information security breach in respect of Shared Information or otherwise, Councillors responsible for the security of that particular information will immediately take steps to contain the breach once it has been identified. If the Council decides that the Information Commissioner's Office should be notified of the breach under Article 33(1) UK GDPR, the Leader of the Council and Cabinet members will also be notified as part of that process. Councillors shall provide reasonable cooperation and assistance in respect of any personal information security breach.

7.5. Once the breach referred to in 7.4 above has been contained, The Council will launch an investigation to establish the reasons behind the breach and will share the outcome of the investigation with the Leader of the Council and Cabinet members.

8. Information Governance

8.1. Before starting any information sharing activity with the Council, the Councillor or Council will consider whether or not to carry out a Data Privacy Impact Assessment (DPIA) as required under Data Protection Legislation to minimise any data protection risks of the information sharing being contemplated and to establish that the proposed information sharing complies with the data protection obligations.

8.2. The Shared Information may not be used by Councillors for any other purposes than those set out in the sharing schedule of Annex 1.

8.3. Where possible and to the extent that it does not conflict with any of the other provisions set out in this document, Councillors shall ensure that any Personal Data, Sensitive Personal Data and Special Categories of Personal Data and Criminal Conviction Data contained within the Shared Information is anonymised.

8.4. In accordance with the Councils data protection policy, Councillors shall implement appropriate technical and organisational measures to maintain the quality and integrity of the Shared Information held by it, having regard to any specific requirements set out under the heading “security requirements” of the sharing schedule of Annex 1.

8.5. Councillors must ensure that the Shared Information is processed securely and, as a minimum, shall adhere to the Council’s information security policy and the “security requirements” set out in the sharing scheduled of Annex 1.

8.6. Where possible, Councillors shall ensure that the information is shared using compatible datasets and that any Shared Information is recorded in the same way by Councillors.

8.7. Where Councillors rely on consent as the condition for processing personal data then withdrawal of consent means that the condition for processing will no longer apply. Where information is shared with the Council and withdrawal of consent applies, you must communicate to the Council without due delay. When withdrawal of consent is received, processing must cease as soon as possible.

8.8. No Councillor should process or otherwise transfer any of the Shared Information outside of the United Kingdom without the written approval of the Council.

ANNEX 1 - What information is being shared

Schedule of Processing, Personal Data and data Subjects

Description	Details
Subject matter of the processing	Personal information can be shared between the Council and Councillors for example, to raise concerns from residents of Rushcliffe Borough.
Duration of the processing	Until Consent is withdrawn or there is no longer a purpose for processing the data.
Nature and purposes of the processing	• To provide advice, if you request it • To investigate any issues or concerns you may raise with me • To find out about your involvement with any other public authorities, if you ask me to • To prevent or detect fraud or other crime
Type of personal data	• Name • Address • Telephone number • Email address • Photographs • Any other details regarding your personal circumstances that you choose to provide to me to help • deal with your query (including details about another person who has asked you to act on their behalf)
Categories of data subject	• Residents living in the Rushcliffe Borough Area. • Projects or planning applications
Plan for return and destruction of the data once processing is complete	All personal shared data must be disposed of securely once processing is no longer required.
Security Requirements	Electronic exchange - All information transmitted across public networks within the UK or across any networks overseas must be sent by secure email which meets UK central government's connection standards or be encrypted using appropriate software (e.g. Microsoft 365, Egress Switch, Cryptshare, etc.)

	• Passwords must be sent separately to the information exchanged and must provide the correct level of security taking all factors into account, including the nature of the data being shared. Passwords must be changed regularly, and Councillors respective password arrangements will include provisions to avoid the use of weak or predictable passwords. • Personal exchange of materials for meetings - Information may be hand delivered or taken in hard copy providing it securely contained within a blue locked bag or similar locked bag or container.