Disclosure of Special Categories of Personal Data – Elected Members Protocol

Contents

1. Purpose

1.1 The purpose of this Protocol is to outline the acceptable disclosure and use of special categories of personal data by all Councillors within the County Borough of Bridgend.

1.2 Under the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR), the Council must consider a number of aspects when deciding whether to disclose special categories of personal data (sensitive data) to Councillors. These will be identified in this protocol.

1.3 This document also sets out the procedure to be followed when requests are received (either via Freedom of Information, Subject Access or Councillor requests) for access to personal data held by Councillors.

2. The Role of the Councillor

2.1 Councillors have three different roles:

a) they represent residents of their ward;
b) they act as a member of the council, for example, as a cabinet member or member of a committee; and
c) they may represent a political party, particularly at election time.

2.2 Depending on the role the councillor has at any one time, under the DPA, the Council may have a duty to disclose special categories of personal data to them. In doing so, it will be necessary to restrict the use of any such information provided for specific purposes.

2.3 The relevant Councillor must on each occasion read and agree the disclosure of special category data checklist prior to them being given any data (Appendix 1). A record of these requests will be kept by the relevant Directorate.

3. Definition of special categories of personal data

3.1 Under the DPA, special categories of personal data are defined as an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health;
- sexual life or sexual orientation;
- biometric data

4. Disclosure to a Councillor representing local residents

4.1 The Council does not generally have to get the express consent of an individual to disclose personal data to an elected member, as long as:

- the elected member represents the ward in which the individual lives;
- the elected member makes it clear that they are representing the individual in any request for their personal information to the Council; and
- the information is necessary for the purposes of, or in connection with, the action reasonably taken by the elected member in response to the individual's request.

4.2 If a Councillor has agreed that they are asking for special categories of personal data (see 3.1) then Appendix 1 **must** be completed prior to the Councillor receiving the information from the Council.

4.3 In most cases the individual would reasonably expect the Council to disclose their personal data to the elected member and disclosure should take place. There may be occasions when it is advisable for the Councillor to get an individual's signed written consent. Circumstances when it would be advisable to obtain signed consent would be where the data is highly sensitive and the instructions to act on behalf of the constituent are not very clear. Councillors and Council staff will need to exercise their judgment on a case by case basis and work together to identify those cases where acting upon implied or verbal consent alone may expose the Council or the Councillor to a subsequent complaint of poor data handling.

4.4 When providing personal information to the Councillor, the Members Code of Conduct is clear that Councillors must not further disclose confidential information without the explicit consent of a person authorised to give such consent or unless required by law to do so.

4.5 Personal information will only be provided to a Councillor to help the individual and must not be used for any other purpose. They must keep this data secure at all times.

4.6 The Council will not give Councillors access to any databases as each request for data must by assessed on a case-by-case basis.

4.7 Where the Councillor receives a copy of the special category data the Council must ensure at all times that the data is being kept securely and not shared inappropriately.

5. Disclosure of Information where the request comes from an individual other than the data subject.

5.1 There may be circumstances whereby the elected member is instructed by a constituent to seek disclosure of personal information which will include information about a **different constituent**.

5.2 Information can only be disclosed in these circumstances provided:

(a) The elected representative is acting in connection with the discharge of their functions as representative
(b) The processing is carried out pursuant to a request made by an individual who is not the data subject to take action on behalf of the data subject or any other individual
(c) The processing is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative pursuant to that request.

AND

It is carried out without the explicit consent of the data subject because:-

(i) In the circumstances consent cannot be given by the data subject,
(ii) In the circumstances the elected representative cannot reasonably be expected to obtain the consent of the data subject;
(iii) Obtaining the consent of the data subject would prejudice the action taken by the elected representative, or
(iv) It is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

5.3 **The onus to be satisfied that the above conditions are met is on both the elected member and the Council. If the elected member is not in a position to satisfy the conditions then they should not submit a request. If the Council is not satisfied the conditions are met they should not release the information.**

6. Disclosure to a Councillor as a Cabinet Member

6.1 The Council can disclose special categories of personal data to a councillor if they need to access and use the data to carry out official duties as a Cabinet Member. This may allow access to information across a number of wards in line with their portfolio responsibilities.

6.2 The cabinet member must specify the purposes for which that information may be used or disclosed on a case-by-case basis.

6.3 Where the Cabinet Member is able to take a copy of the personal information away from the premises the Council must ensure that the data is being kept securely and not shared inappropriately.

7. Disclosure to a Councillor when representing a political party

7.1 The Council should not normally disclose personal information to elected members for political purposes without the consent of the individuals concerned.

7.2 There are two exceptions to this:

- Sets of personal information which the Council is required to make public, for example, lists of some types of licence holder
- Personal information presented in an aggregated form and does not identify any living natural individuals. For example, Council Tax band information or statistical information. (However, there would be a breach of the DPA if personal information was released in an apparently anonymised form which could then be linked to the individuals concerned, for example, by comparing property data with the electoral roll.)

8. Requests for Personal Data held by Councillors

8.1 Should any request be received by the Council for information held electronically on a Councillor's bridgend.gov.uk email account, the request will be administered by the Council's Information Team. The Councillor will be notified and a discussion will take place regarding where the information is held. The retrieval of the information will be undertaken on behalf of the Councillor with the information being retrieved by officers.

8.2 If a request for such information is received, Councillors should be aware that it would be a breach of the Members Code of Conduct and a criminal offence to delete any information held that falls within the parameters of the request.

8.3 Any hard copy information will be will be administrated in the same way as electronic information.

9. Risk Management, Record Keeping and Co-operation

9.1 The sharing of special categories of personal data should always be undertaken with due care and diligence. At all times the sharing of such data should be undertaken with the understanding that a heightened standard of care and attention is to be applied when data is not only personal but sensitive in nature.

9.2 This protocol is based upon the provisions to permit the processing of special categories of personal data outlined in Part 2 Schedule 1 of the Data Protection Act 2018. It represents a common sense approach to the sharing of special categories of personal data without the need to obtain explicit written consent.

9.3 **This protocol does not however represent a free flow of information without any safeguards which are all detailed above. The Data Protection Act is clear that information processing must be necessary, time bound and must be limited to specific purposes.**

Examples that this protocol and the form at Appendix 1 seek to address:

A Councillor receives consent from a constituent to complain about an issue. Verbal consent is provided for the Councillor to take up the issue with the Council and access special categories of personal data 'x'. The Council accepts it is a valid request and copies and provides a whole file which contains information 'x' and 'y'. The Council has provided

information beyond the scope of the consent and has therefore breached the Data Protection Act.

A Councillor receives consent from a constituent to complain about an issue. Verbal consent is provided for the Councillor to take up the issue with the Council and access special categories of personal data 'x'. The Council accepts it is a valid request and copies and provides information 'x'. The Councillor having dealt with the complaint issue for their constituent then uses the data for other purposes during a debate about a similar issue without first speaking to the constituent again. The Councillor has exceeded the extent of the consent provided and has breached the Data Protection Act.

9.4 It is important therefore to have an open dialogue between the individual and the elected representative and the elected representative and the Council. Each individual should be clear as to the boundaries of the consent they have been provided and the extent to which disclosure is necessary. There is an expectation of cooperation, advice and assistance to ensure that unauthorised data sharing does not occur.

9.5 This protocol does not mandate that those involved in the sharing of special categories of personal data maintain records and written consents over and above the checklist contained at Appendix 1. It is however anticipated that there will be circumstances that warrant additional care to be taken and a clear record kept.

9.6 An elected member will receive their instructions in a variety of ways – email, telephone or at a surgery for example. The instructions to act on the individual's behalf may be provided at a time of crisis / upset for the constituent, at short notice requiring immediate action and during a brief conversation in a public place. The elected member should consider the sensitivity of the data they are being requested to access and how clear their instructions to act are. This protocol does not mandate the elected ember to keep their own records but to use their judgment as to the circumstances whereby it would be beneficial to have such a record should there be a subsequent complaint.

9.8 An elected member should only retain personal data for as long as the individual's issue is active. This will be a matter of judgment for the elected member based on their knowledge and experience of working on behalf of their constituents.

9.9 Members should be aware that they need to arrange for appropriate security to protect personal information. They must take into account the nature of the information and the harm that can result. They should consider what technical and organisational measures, such as use of passwords, procedures are appropriate to keep the information safe. The Council must also take appropriate measures in the same way.

9.10 The DPA contains a number of criminal offences, including:

- Failure to register as a Data Controller with the Information Commissioner's Office when required to do so
- Procuring unauthorised disclosures of personal information
- Unlawfully obtaining, or disclosing, personal data
- Alteration of personal data to prevent disclosure to a data subject
- Re-identification of de-identified personal data without the consent of the data controller

Appendix 1

Bridgend County Borough Council

Disclosure of Special Categories of Personal Data Checklist

Councillor Name:	
Ward/Portfolio:	
Representing:	

For Bridgend County Borough Council to provide a Councillor with special categories of personal data of an individual the Councillor must first agree on the following points:

Description	Tick to agree
1. I am representing the ward/portfolio in which the individual lives	
2. Prior consent has been given by the individual for me to obtain this data on their behalf	
3. I will only use this data for the purpose of this case	
4. I will ensure that I keep the data secure and will not intentionally share the data with any unauthorised parties	
5. I understand that I may be personally liable for negligently or misusing personal data	
6. I will immediately report any misuse of this data to the Council's Data Protection Officer	

Required Details

Why is this information/data needed?
What are you going to do with the information/data?
Who will you be sharing the information/data with?

Signed: **Date:**