Data Protection & Information Use

Policy

Information Management Team

V1.0 Final

Version

Date	Version	Status	Notes
20 August 2018	0.1	Draft	Author – Jaimie Taylor, Information Manager
27 August 2018	**1.0**	**Final**	Approved by the IGG 27.08.18

1. **Introduction:**

"A person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority." (Section 1(1) of the Freedom of Information (Scotland) Act 2002);

"Everyone has the right to respect for his private and family life, his home and his correspondence." (Article 8(1) of the European Convention on Human Rights).

1.1 The two passages quoted above serve to highlight the conflicting demands which can be placed on the information held by public sector bodies such as Scottish Borders Council. Freedom of information requires us to be open and transparent with our stakeholders, whereas human rights and data protection considerations mean that not all information can properly be released, and the Council is instead obliged both legally and morally to hold that information securely and in confidence to ensure that only those with a legitimate need to see that information are able to do so. This document sets out a high level policy describing how the Council will approach the collection, use, disclosure and disposal of information.

1.2 This policy is binding on Council services. Arms Length External Organisations will be expected to adopt similar rules to these in terms of their own handling of information.

1.3 This policy is primarily concerned with personal data, i.e. information relating to identifiable living individuals, and its main focus is to explain to external stakeholders what the Council will do with that information. The Council also has a governance framework under which binding rules on the Council's internal use of all information can be issued; these rules are primarily concerned with how the Council manages information internally.

1.4 In terms of explaining what the Council does with information, this Policy should be read alongside the privacy statement published by the Council.

2. **Strategic position on information:**

2.1. Information is a corporate asset. The Council accordingly adopts the following points of principle in relation to the information which it acquires or creates:

2.1.1. The Council recognises that it holds information as custodian for the people of Scottish Borders Council.

2.1.2. The Council recognises the importance of the information it holds, in terms of its impact on and relevance to the people of Scottish Borders Council, its intrinsic value in assisting the Council perform its public functions, and its potential value to future generations as a historical and archival resource.

2.1.3. If information relates to the private or family life of an individual, the Council will as a general principle seek to keep that information confidential and will resist releasing it where possible. This policy sets out the circumstances under which the Council may or will release information of this type, who it may release it to and why.

2.1.4. If information does not relate to the private lives of individuals, then the Council will as a general principle consider that the information be treated as public.

2.1.5. Information held by the Council will be treated in accordance with the rules set out in this policy and in accordance with Procedural Rules issued in conjunction with it. This policy is accordingly the Council's explanation of the way in which it handles personal information.

3. **What we use personal information for:**

3.1. The Council uses the information which it holds for the primary purpose of providing relevant local authority services to service users. For most (but not all) services, this is on the basis of the service user agreeing to provide information to the Council in order to allow the Council to provide those services. Some regulatory or protective functions require to be carried out without the consent of those affected.

3.2. The Council will also use the information it holds for the prevention and detection of crime where this is relevant. We will not ask for consent for this, or for any other area where the Council would be proceeding whether consent was given or not, but will alert people to the fact that we will be proceeding without their consent. (This would not apply to some regulatory activity such as directed surveillance).

3.3. The Council may wish to offer someone additional services, we may wish to (or be legally obliged to) share information with other public bodies, either to improve service delivery to the individual or for purposes such as crime prevention. We may need to use information for research purposes with a view to improving how services are delivered in future or in order to assess future levels of demand. Where the Council wishes to make such secondary uses of the personal data it is provided with, this will be made clear to the individuals through the Council's privacy statement as published from time to time.

3.4. All secondary uses of personal information must comply with the principles set out in this Policy.

4. **Principles for secondary uses and disclosure of personal data:**

4.1. Decisions on whether or not the Council will seek to make a secondary use of personal information or will release personal information to an external agency will be informed by the following priorities:

4.1.1. Is it lawful for the Council to do so?

4.1.2. Is the release of identifiable information necessary to achieve a legitimate public objective? (If the objective can be achieved without releasing personal information, the alternative method should be pursued instead).

4.1.3. Is this objective one which the Council should, as a matter of policy, be pursuing or assisting another body in pursuing?

4.1.4. Would the individuals affected have a reasonable expectation that their details would not be used in the way proposed? (Such reasonable expectations would require a very significant public benefit to justify the information release. This relates to what individuals were advised might happen to their details, including what this policy says might happen to them).

4.1.5. Is the release of the information proportionate to the benefits to be achieved? This means that there should be a relationship between how privacy-intrusive the measure is and how significant the benefit to be achieved is. Privacy intrusiveness is dependent on a number of factors such as: how many people are affected; how much information about them is released; the nature of the information in question; how widely the information will be shared; how long it will be shared for; and the degree to which affected individuals may or may not be able to opt out of the process. If the benefits can be achieved with less privacy intrusion, or if major privacy intrusion will produce only minor benefits, then what is proposed will be a disproportionate interference with privacy and will be resisted.

4.2. In reaching a decision on any proposed secondary use or external disclosure, Council officers will when relevant make full use of data protection impact assessments, and will follow best practice as published by the (UK) Information Commissioner in relation to these data protection impact assessments (including best practice as to when such an assessment is required and the level of detail required in this assessment). Secondary uses or external disclosures will only proceed where the outcome of any data protection impact assessment is favourable.