Appendix 2(c) # DATA PROTECTION PROCEDURES

3. How to share information internally or with partner organisations using an Information Sharing Agreement on a planned basis, or using a non-disclosure exemption on an ad hoc basis.

Introduction

This guidance must be used when Belfast City Council (BCC) is considering sharing personal data internally between departments or with external partner organisations on a planned basis. It also contains guidance on how to obtain and disclose personal data on an ad hoc basis using the non disclosure exemptions.

BCC is required, to share and obtain personal data when there is a necessity and a pressing need to do so. Sharing will involve personal data and for the purposes of this guidance document personal data will be referred to as information.

Information is an extremely valuable and a vital asset to BCC in managing its day to day obligations. By working closely internally and with external organisations, BCC can enhance the service it provides and increase public safety. Achieving this will often involve the sharing of information.

BCC must comply with the rules and obligations specified within the Data Protection Act 1998 and this should not be seen as a barrier to sharing of information, but that it provides a framework to ensure personal data is shared properly and lawfully.

Purpose of guidance

This guidance will set out the rules and pathway for information sharing. It is important that departments understand when, why and how they should share information confidently and lawfully. The following points address the reasons for this guidance.

- To guide BCC on how to share personal information lawfully with internal departments and partner agencies.
- To explain to staff involved the security and confidentiality issues together with the principles of information sharing.
- To increase awareness and understanding of the key issues.
- To emphasise the need to develop and use Information Sharing Agreements.
- To support a process that will monitor and review all information sharing.
- To encourage the sharing of information.
- To protect BCC and any partner agencies from wrongful use of personal data.
- To identify the legal basis for information sharing.

Sharing of personal data is restricted solely by the Data Protection Act 1998 and includes that held in electronic and manual format including, CCTV.

The guidance will also explain how to address security and confidentiality, together with the main elements of information sharing. Staff will be in a position to understand the key points involved and manage the proper transfer of information while protecting against unlawful or excessive sharing.

BCC will promote staff awareness in this area, which will be delivered by the Information Governance Unit as part of an overall Data Protection training programme.

There are three main areas in which sharing will take place as follows:-

- Internal sharing between Belfast City Council Departments / Sections / Units
- External sharing with partner organisations either statutory or non-statutory
- Disclosing and obtaining information on an ad hoc basis from other organisations

General Principles

The principles outlined in this document are recommended as good standards of practice and legal requirements that should be adhered to by BCC. This sets the core standards applicable to the council and should form the basis of all Information Sharing Agreements.

BCC and partner organisations are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and their staff are properly trained to understand their responsibilities and comply with the law.

Internal Sharing

Internal BCC departments / sections / units will process personal data in electronic and paper format for a number of different purposes to meet their specific needs. In certain circumstances there will be a requirement to share personal data between each other and this must be carried out in a safe and proper manner. Only proportionate and relevant information should be shared and on a need to know basis.

Common sense should be applied when internal sharing is considered as there will always be a need for regular contact between departments / sections / units to discuss a common case, complaint, and customer or to confirm basic personal data e.g. address and DOB details. This can be described as low level sharing, which is mainly carried out to ensure accuracy, relevancy and the updating of information. If routine interaction and contact was not permitted for this type of sharing there would be an obvious impact on the delivery of Council business. However, the following process should be used when **detailed copy** personal data is being sought between departments / sections / units. Necessity is the key in these instances and each sharing request should be carefully examined.

In most instances, internal departments / sections / units will not have direct access to each other's specific electronic or manual information systems. Therefore, it is important the department / section / unit seeking the information should provide a record of the request for access to the information they require. It is also essential to provide the reason why the information is needed and state the purpose for which they intend to use it.

This can be carried out by completing the internal personal data sharing request form Template 3.1.

The form will provide appropriate background information, therefore allowing the department / section / unit who hold the data to make an informed decision on whether to share it or not. Page 1 of this form will be completed by a member of staff seeking the information. Page 2 of this form must be completed by a member of staff holding the information. Both parts must be authorised by a line manager or deputy.
The use of this form will provide reassurance between departments / sections / units that any requests for access to the information they hold are legitimate and valid.

If the sharing involves providing a staff member direct access to an electronic or manual information system, then suitable access levels must be agreed by the holding department / section / unit to ensure only the appropriate amount of information is available.

The completed original form must be retained by the requesting department, and a copy held by the receiving department.

External Sharing

BCC must share information for a variety of important reasons between statutory and non-statutory organisations when the need arises. This is usually carried out when regular sharing is planned and under a formal structure.

This type of sharing carries additional risks as BCC information will be handed over to an outside body, albeit for a lawful purpose. Despite this, there has to be a necessity to share the information and the process carefully documented and controlled within a formal information sharing agreement (ISA).

The balance between the need to share information, while protecting the confidentiality of BCC data can be difficult to meet. Confusion can occur as to the level of protection BCC must apply to the information they retain and use. This can lead to important information being withheld from partner organisations who have a valid and urgent need to know while conversely, excessive and non relevant information is released.

If a BCC department is approached or identifies a need to share information with a partner organisation, the generic BCC Information Sharing Agreement form should be completed. This template will cover all the main points involved by providing a level of security and formality to the process. The template information sharing document is held by Information Governance Unit and a copy can be obtained together with advice and guidance on its completion.

Proportionality

The information that BCC share must be proportionate and should be the minimum amount needed to achieve the purpose of any agreement. It may be possible after consultation with the partner organisation to use information that does not identify individuals (anonymised data). This can be decided on a case by case basis.

Legislation / Lawful basis for processing

The principal legislation concerning the protection and use of information is as follows:-

- Human Rights Act 1998 (article 8)
- The Freedom of Information Act 2000
- Data Protection Act 1998
- The Common Law Duty of Confidence
- Computer Misuse Act

The Data Protection Act demands a lawful basis for disclosure to ensure the main objective of the sharing can be achieved.

All ISAs must clearly identify the legal basis being relied upon and this may vary on the nature of the actual information to be shared, however it is essential BCC do not operate beyond its powers. No one piece of legislation will cover every situation but if in doubt, further advice can be provided by Legal Services or the Information Governance Unit.

Information covered by this procedure

All personal data and sensitive personal data as defined within the Data Protection Act 1998.

The term 'personal data' refers to **any** data held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that data. The term is further defined in the DPA as:

- Data relating to a living individual who can be identified from those data;
- Any other information, which is in the possession of, or is likely to come into the possession of the data controller (person or organisation collecting that information).

The DPA also defines certain classes of personal information as 'sensitive data' and the Act places additional conditions on the data controller with specific reference to how it processes that information.

- Race or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a Trade Union
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Proceedings for any offence committed or alleged to have been committed.

Schedules

The schedules 2 & 3 mentioned within the DPA are lists of conditions that **must** be met when BCC is processing personal and sensitive personal data. Advice and guidance on the relevant conditions to apply in each case should be obtained from IGU.

Consent

Consent can be an overriding factor when personal data is considered for sharing, which should be explored at the very outset to consider if it is appropriate for the purpose of the agreement. If consent is sought, it must be freely given and fully understood by the person involved and must be explicit if the data is sensitive. Consent has to be signified by some communication between the organisation and the data subject.

Where an organisation has a statutory obligation to disclose personal data, then the consent of the data subject is not required, but the data subject should be informed that such an obligation exists.

After initial consideration, it may be identified that seeking consent is not an option and by doing so will prejudice the purpose of the sharing. If an assessment is made by the core organisations involved that consent is not an option nor should be sought, then background decisions must be documented.

It is also possible that a data subject may object or withdraw consent to the processing of their personal information. In this case, the processing can only continue where an applicable Data Protection Act
If the sharing is reliant upon consent as the sole condition for processing personal data within the agreement, then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to each organisation involved and processing cease as soon as possible.

Corporate and individual responsibilities when sharing

The need to share information will usually commence after a certain issue arises or an area of mutual concern between partner organisations is identified. Initial discussions will take place and an agreed manner on how to proceed will be developed. However, the overall responsibility to maintain the security and confidentiality of information, either in manual or electronic format is vital.

It will be the responsibility of each Head of Service / Director to ensure that any current and future sharing arrangements are properly managed within their area of responsibility and this guidance / procedure followed. Before a Department signs off an information sharing agreement, the Head of Department must forward a copy to the Information Governance Unit for review and approval.

BCC must identify and list within each agreement the designated staff that will be responsible on a day-to-day basis for the information sharing. It is also essential that details of the actual information shared are retained by the department involved. It is not acceptable to share information without keeping a record of what was handed over.

BCC has an overall responsibility to audit the compliance of any Information Sharing Agreements they are part of. This can be completed either independently or in co-operation with the other organisations on an annual basis by the department involved and / or by the Information Governance Unit.

If a breach of confidentiality or security occurs, **each party involved must be informed immediately**. This must be carried out by the designated officers. BCC Information Governance Unit must also be informed as soon as possible to establish the nature of the breach and any follow up action required. (See procedures on what to do in the event of a Data Breach).

Staff must uphold the general principles of confidentiality, follow the guide-lines set out in the agreement and seek advice when necessary. Every individual should be aware that any violation of privacy or breach of confidentiality maybe unlawful and a disciplinary matter that could lead to investigation. **Criminal proceedings might also be brought against that individual**.

Constraints / Restrictions on further use

All information contained within an ISA, either personal or non-personal, must only be used for the purpose specified at the time of disclosure and will be defined in a relevant agreement.

Any further use made of this data will not be lawful or covered by the ISA unless obliged under statute or under the instructions of a court. Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity. If in doubt, the information's original owner should be consulted.

The information shared as part of an agreement should not be disclosed to any other third party without the written consent of Belfast City Council or core partner organisations listed within the agreement.

In certain circumstances it may be necessary to engage the services of a designated organisation that sits outside the core partners. If this is identified and necessary, then a decision must be made on the extent of information that can be shared with them.

Full agreement between all partner organisations involved is vital and the template from must be used. This will be forwarded and signed by a nominated person within the designated organisation, which places security and confidentiality obligations on them. Details of this addition will be added to the ISA if required.

Security / Information Exchange

BCC works to the principles of the British Standard ISO 27001, the Standard for Information Security Management. Compliance or a similar level of compatible security should be sought from any partner organisation involved to confirm a suitable level of security is in place to process BCC information. There may be instances whereby a partner organisation will not have a specific security classification in place. If this is identified, **then BCC must carefully consider whether to proceed or not**.

In most instances information sharing agreements will involve the transfer of information between the partner organisations. This should be performed by way of secure electronic transfer or hand copy delivery.

A process must be agreed between the organisations involved and must be completed with due regard to the seventh principle of the DPA. "*That appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".*

Ad hoc disclosures under the non-disclosure exemptions

Ad hoc disclosures of personal data to external organisations are not compulsory except in cases where BCC is served with a Court direction requiring it to disclose the information requested or when a specific piece of legislation obliges BCC to disclose. However, the two main exemptions that apply to the Council enabling it to voluntarily disclose information are Section 29(3) and 35(2) of the Data Protection Act 1998 (prevention & detection of crime and in connection with legal proceedings).

The disclosures work in two ways:-

1) When an outside organisation is seeking information held by BCC

Such disclosures should only be made if the requesting organisation requires personal data relating to a specific matter and they must provide suitable information to satisfy BCC that failure to release will harm their purpose and necessity is the key.

The request must be in writing and if any member of staff receives a telephone call from the external organisation, they are not obliged to release information by this means. Most requesting organisations have a dedicated request form, which will include:

- a statement confirming that the information requested is required for the purposes covered in Section 29 or 35;
- a brief outline of the nature of an investigation or reason for seeking the information;
- the data subject's role in that investigation or purpose;

- the signature of the investigating officer.

There is no such thing as a Data Protection emergency (except where someone's life or health may be at risk or the police require the data urgently to intervene in a crime). If life is endangered and it is vital that police or another organisation obtain the personal data immediately, the telephone can be used. If in doubt, seek immediate guidance and advice from a line manager.

2) When BBC is seeking information held by an external organisation

Such disclosures should only be made when BCC requires personal data relating to a specific matter and they must provide suitable information to satisfy the external organisation that failure to release will harm its purpose and necessity is the key.

The request must be in writing and BCC has a dedicated request form for this purpose, which will include:

- a statement confirming that the information requested is required for the purposes covered in Section 29 or 35;
- a brief outline of the nature of an investigation or reason for seeking the information;
- the data subject's role in that investigation or purpose;
- the signature of the investigating officer.

Template non-disclosure request from can be obtained from RMU, along with advice and guidance on its completion.

Quality of Information

BCC must ensure that any Information shared is of high quality and needs to be fit for the purpose it is to be used. It must be complete, accurate, up to date and without this, any decision made on the information shared may be flawed leading to inappropriate actions taken as a result. All organisations are expected to give undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared. In essence BCC must be able to stand over any information that it will share.

Training

BCC staff who are involved in the sharing of information are expected to receive a level of training in the use and management of the agreement. This will enable them to undertake their duties in a confident, efficient and lawful manner. This can be provided by the Head of Department and in conjunction with Information Governance Unit.

Template 3.1 – Internal Information Sharing Agreement

Template 3.1

Internal Belfast City Council Personal Data Request Form
(To be used when sharing between Department / Section)

To – *(List the name of person within the department / section)*

Department & Address – *(List address of internal department / section)*

This is a request for access to personal data processed on Belfast City Council's internal information systems where the requesting department / section does not have direct access.

The personal data required will relate to the following individual:-
(Include name, address, DOB and any other identifying details).

Details of the personal data that I require are as follows:-
(Describe the data sought)

I require the personal data for the following purpose:-
(State exactly why this data is required and provide as much details as possible, provide details of prejudice or harm caused if the information is not disclosed and any legislative powers you are relying upon)

Signature of requesting member .....

Date..... **Department**.....

Signature of authorising member.....

Date..... **Department**.....

To be completed by the receiving department / section.

State if the personal data is to be released to the above department / section. If the data is to be withheld, an explanation must be provided as to the reasons for this decision. **If direct access is provided for staff to use an information system, please provide details.**
(State if the data can be released or not. If released, list the details. If not, then include the reason why it is withheld.

The personal data has been approved for release	**Yes / No**

Signature of reviewing member .....

Date..... **Department**.....

Signature of authorising member.....

Date..... **Department**.....