**Appendix 1**

Belfast City Council

# DATA PROTECTION POLICY

## 1. Policy Control

| | |
|---|---|
| **Organisation** | Belfast City Council |
| **Title** | Data Protection Policy |
| **Author** | Robert Corbett, Records Manager |
| **Owner** | John Walsh, Town Solicitor |
| **Review date** | November 2016 |
| **Location of document** | Interlink / website |
| **Approved by** | |
| **Approval date** | |

## 2. Contents



## 3. Introduction

Information is a valuable asset. Like any other business asset it has a value and must be protected. This policy sets out the council's approach to processing personal data under the Data Protection Act 1998.

## 4. Scope

This policy applies to everyone who has access to the Council's information, information assets or IT equipment. This may include, but is not limited to, employees of the Council, elected Members of the Council, temporary workers, partners and contractual third parties.

All BCC staff that use or have access to Council information must understand and adopt this policy and are responsible for ensuring the security of the Council's information systems and the information that they use or handle.

The Act applies to **personal data** contained within:

- Electronic and paper based information systems
- Email
- Backup/archive systems
- CCTV recordings
- Microfiche
- Card indexes

## 5. Legislative Context and Regulation

The Data Protection Act (DPA) 1998 is based on a European Directive and was introduced to protect the personal privacy of individuals. It regulates the use of personal data processed on computers and in paper filing systems. It provides rights for individuals and places legal obligations on organisations as to how they gather, retain, use and protect personal data. It is essentially a rule book for the processing of personal data.

**Regulation**
The Act is regulated by the Information Commissioner (ICO), which is an independently appointed post answerable directly to Parliament. A Deputy Information Commissioner for Northern Ireland and Scotland is responsible for compliance within this jurisdiction.

The ICO has the powers to:

- Carry out assessments (examine how a DPA matter was dealt with by BCC);
- Issue information notices (compel BCC to provide it with information);
- Issue enforcement notices (compel BCC to take a certain course of action);
- **Prosecute for criminal offences** committed under the DPA; and
- **Issue monetary fines** to an organisation of up to £500,000 for breaches of the Act.

**Notification**
The Data Protection Act 1998 places a legal obligation on the Data Controller (BCC) to notify the Information Commissioner of the lawful purposes why it is processing personal data. This is completed annually by the Information Governance Unit, and failure to notify is a criminal offence.

The Information Commissioner has allocated BCC with a notification reference number – **ZA104779**. Details of this notification can be found and viewed by accessing the Information Commissioners' website at www.ico.gov.uk and click on Register of Data Controllers and then search register.

Personal data is processed for the purposes listed within its notification to the ICO and for the use of BCC to fulfil its statutory obligations. **Personal data should not be used by any member of council staff for private or individual purposes, which is strictly forbidden.** Any inappropriate or unlawful use by council staff may leave that person liable to internal disciplinary action and or criminal proceedings.

The Act also places a high level of corporate responsibility on BCC who may be subject to enforcement action for any compliance failings. **Failure to meet the terms of any enforcement action may be a criminal offence.**

It is essential that all BCC staff who handle personal data are in a position to generally explain (if asked) to an individual the purpose or purposes of why their department / section / unit hold and use data.

**Rights available to a data subject**
The Data Protection Act 1998 provides a number of rights, relating to the following:

- Prevent damage or distress;
- Stop direct marketing;
- Provide the logic to automated decisions;
- Seek compensation; and
- Rectify, erase and block.

These must be referred in writing to the Data Controller (BCC) who has a legal obligation to address within a specified time frame.

## 6. Corporate Risk

Compliance with the Data Protection Act and associated legislation has been identified as a key corporate risk and as such requires robust management. The Council will promote best practice by developing safe and secure data handling via documented procedures and guidance. Failure to properly manage the Data Protection obligations may leave the Council in breach of the Act and open to legal action by a data subject and / or the Information Commissioner.

## 7. Definitions

Key definitions from the Data Protection Act which staff should be aware of:

| Term | Definition | Example |
|---|---|---|
| **Personal data** | Data relating to a living individual who can be identified from that information or from that data or other information in the possession of the Data Controller | Includes name, address, national insurance number, personnel files, marriage records, complaints made to BCC etc |
| **Sensitive Personal Data** | Personal data consisting of information relating to racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life or criminal proceedings or convictions | |
| **Data Controller** | A person who alone or jointly with others determines the purposes for which and the manner in which any personal data are or are to be processed | In this instance, BCC is the data controller |
| **Data Subject** | An individual who is the subject of personal data | Includes members of the public and internal staff |

| Term | Definition | Example |
|---|---|---|
| **Data Processor** | Any person (other than an employee of the data controller) who processes personal data on behalf of the Data Controller.<br><br>This will be carried out on BCC's behalf and under its instructions and control. | Could be an outside company performing a specific function for BCC e.g. a recruitment process or a consultant. |
| **Processing** | Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. This includes organising, adapting, altering, retrieving, disclosing, and destroying | |
| **Relevant Filing System** | A set of information about individuals, structured either by reference to individual or by reference to criteria relating to individuals | |
| **Third Party** | An individual other than the Data Subject, Data Controller or Agents of the Controller | |

**Other definitions**

| Term | Definition | Example |
|---|---|---|
| **Records Liaison Officer (RLO)** | RLO will manage the administrative and liaison aspects involved in the processing of subject access requests submitted to the department. | |
| **Decision-makers** | Make decisions on the exact amount of personal data to release in relation to a subject access request. Apply exemptions if personal data is to be withheld and manage any complaints impacting on compliance with the Data Protection Act 1998.<br><br>These individuals will also take decisions relating to other aspects of compliance with the Data Protection Act 1998 focusing on Information Sharing, Data Processing and the application of Non-disclosure exemptions. | |
| **Subject Access Requests (SAR)** | Section 7 of the DPA provides a legal gateway for an individual to seek access to personal data. This is a fundamental right and is routinely referred to as a subject access | In practice, this can be done by an individual making a SAR, which can be received by any member of BCC. It is essential that Council staff recognise this type of request and inform their RLO as soon as possible as the legal time |

| Term | Definition | Example |
|---|---|---|
| | request. This gives individuals the right to be told what personal data BCC is holding about them and to have that data communicated to them in intelligible form, which is subject to any exemptions | frame for compliance is **40 calendar days**. The request must be **in writing** (including fax and email) but cannot be accepted by telephone. |
| **Data Sharing** | This involves the sharing of personal data between internal BCC departments and with outside partner organisations which can be vital to meet BCC's statutory responsibilities. The sharing of personal data can assist BCC by supporting its provision of services to members of the public and additionally work in partnerships to reduce and prevent criminal activity. | Sharing between statutory agencies to reduce Anti Social Behaviour within a specific area. |
| **Data breach** | When personal data held by BCC is lost, stolen, subjected to unauthorised or unlawful access, unlawful use, or disclosure. | Data breaches can occur in a number of ways with some examples listed below:-<br><br>• lost or stolen laptops, removable storage devices, or paper records containing personal information;<br><br>• databases containing personal information being illegally accessed by individuals outside of the organisation;<br><br>• employees accessing or disclosing personal information outside the requirements or authorisation of their employment;<br><br>• paper records stolen from insecure recycling or waste bins and devices to be destroyed that have not been securely cleaned;<br><br>• mistakenly providing personal information to the wrong person, e.g. by sending details out to the wrong address; and<br><br>•an individual purposely deceiving BCC staff into improperly releasing personal data. |

## 8. Roles and Responsibilities

**Town Solicitor**
The Town Solicitor has overall responsibility for preparing policies and strategies for approval, guidance and advice, notifications to and dealings with the Information Commissioner and monitoring and compliance in relation to matters within the scope of this policy.

**Information Governance Unit**
The role of BCC's Information Governance Unit (IGU) is to assist the Council with its overall Data Protection compliance. This unit is responsible for providing advice, guidance and awareness training to all staff on matters covering the statutory obligations found with the Data Protection Act 1998.
The IGU is the first point of contact for all queries or matters from internal staff and members of the public relating to the Data Protection legislation. It will also be the central hub for the monitoring of subject access requests (SAR) made to BCC and provide a level of quality assurance to all SARs.

**Directors**
Each BCC Department is responsible for the personal data that it processes and must take steps to make certain its data is fit for purpose and processed in line with the principles of the Act. The relevant Head of Service or Director has the responsibility to promote proper management, security and supervision of the personal data on which his / her department rely upon to perform their Council functions.

**Departmental Record Liaison Officer(s)**
Each BCC Department Director will appoint staff who will act as Record Liaison Officer(s) (RLO). The person who assumes this role will receive appropriate training and must also be aware of the requirements of DPA and have specialist knowledge of information within their Department. The RLO will manage the administrative and liaison aspects involved in the processing of subject access requests submitted to the department. This will include the recording of comprehensive and accurate details onto CRM.

**Departmental Decision Makers**
Each department will appoint members of staff to fulfil the role of Decision Makers (DM). The person who assumes this role will receive appropriate training and must also be aware of the requirements of DPA and have specialist knowledge of information within their Department. The DM is accountable in the decisions he or she makes and has two main functions as follows:

a) Manage the actual processing of a SAR from submission to closure. This will include recovering and reviewing any personal data processed by BCC in relation to the request. Make a decision of the exact amount of personal data to release and apply exemptions if personal data is to be withheld.
b) Manage any complaints received in relation to data subject's rights by providing comprehensive responses within the statutory time frames.

**All staff**
All BCC staff are responsible for ensuring that any personal data is processed in a lawful manner. It is essential that full compliance with the Act is addressed and each staff member has a duty to maintain the integrity of the information and the confidence of the public who have an expectation their personal information is in safe hands. Staff must abide by the following obligations:

- Ensure proper care is taken when gathering, using or disclosing any personal data where it is necessary to meet your departmental functions;
- Take all necessary steps to keep personal information secure and only use it for the purposes intended;

- Personal comments and remarks on manual files or electronic records (including emails) must be appropriate and professional;
- Ensure the personal data recorded is accurate, clear and adequate;
- Avoid accidental unauthorised disclosure by fax, voice, email or other means by double checking and using call back procedures;
- Keep personal data confidential and do not disclose it to any other person unless you are authorised to do so (f in doubt ask your line manager);
- Ensure that any electronic data files or paper printouts containing personal data are disposed of safely and not removed from council premises without appropriate security measures or left in an unsecure area;
- Keep system passwords safe. Change regularly and do not disclose them to anyone;
- Comply with this and other related polices e.g. Records Management Policy, Computer use Policy and Information Security Policy; and
- Attend DPA Training, which is mandatory

**Note – It is imperative that all staff must check and seek the approval of their line manager / supervisor when necessary, before making any disclosure or release of personal data by letter, fax, telephone, email or other means.**

## 9. Policy Statement

Belfast City Council is legally obliged and fully committed to comply with the provisions of the Data Protection Act 1998. The Council must gather, retain and use personal data about living individuals to fulfil its statutory functions and provide council services.

BCC will follow lawful practices and procedures on how it manages personal data while respecting the rights, privacy and freedoms of individual members of the public, internal staff, contractors, suppliers of services, customers and grant recipients.

In keeping with the eight principles of the Data Protection Act, Belfast City Council will ensure that personal data:

1. Shall be **processed fairly and lawfully** and in particular, shall not be processed unless conditions within schedule 2 and in the case of sensitive personal data schedule 3 are met (see below)

2. Is obtained **only for one or more specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Shall be **adequate, relevant and not excessive**

4. Shall be **accurate**, and where necessary, **kept up to date**

5. Is **not kept longer** than necessary

6. Shall be processed **in accordance with the legal rights** of the data subjects

7. Shall be held **securely** with appropriate technical and organisational measures taken to guard against unauthorised or unlawful processing of personal data and against accidental loss, damage or destruction.

8. **Shall not be transferred to a country or territory outside the European Economic Area** (defined as EU Member states, plus Norway, Iceland and Liechtenstein) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Lawful Processing**

BCC will ensure that all processing of personal data will be conducted fairly and lawfully and in compliance with the data protection principles listed above. In particular, shall not be processed unless – **(i)** At least one of the conditions in Schedule 2 is met, and **(ii)** In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Summary of Schedule 2 Conditions:

a) Consent has been given in general terms;
b) Non-contractual legal obligations;
c) Vital interests of the data subject;
d) Administration of justice;
e) The exercise of functions conferred by or under enactment;
f) The exercise of any functions of the Crown, a Minister of the Crown, or a Government Department;
g) The exercise of any other functions of a public nature exercised in the public interest;
h) Processing that is necessary for the legitimate interests of the data controller or a third party, except where the processing would cause unwarranted prejudice to the rights and freedoms of the data subject.

Summary of Schedule 3 Conditions:

a) Explicit consent to the specific processing;
b) Vital interests of the data subject, where explicit consent cannot be obtained or has been withheld unreasonably;
c) Processing is necessary for legal proceedings;
d) Administration of justice;
e) Exercise of any functions conferred on any person (including a constable) by or under enactment;
f) The exercise of any functions of the Crown, a Minister of the Crown, or a Government Department;
g) Further conditions have been enacted under statutory instruments – of particular significance to the police service is;
h) Processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

BCC will ensure that it has proper and legitimate grounds for collecting, handling and using personal data. The data will not be used in a manner that would have an adverse or detrimental impact on the individuals concerned unless the law permits. The Council will strive to be diligent and responsible as to how it processes personal data and handle it in a way that any individual would reasonably expect.

**Security**

BCC will provide proper security management, robust access controls, business continuity planning, staff training, compliance auditing and measures to prevent and detect breaches of security. BCC takes this obligation very seriously and all departments work collectively and in conjunction with Digital Services to achieve a high level of information security.

**Information-sharing**

BCC will only share personal data internally and externally when there is a legal basis to do so, while meeting the obligations found within the Data Protection Act 1998 and guidance found within the ICO Code of Practice on sharing personal data. Sharing can take place in the following formats:

- On an irregular ad hoc basis, when BCC may require access to personal data held by another organisation or when the other organisation may seek access to the personal data held by BCC.
- On a regular basis when the sharing of personal data is routinely required between BCC and other organisations to meet their statutory obligations. (e.g. National Fraud initiative, Anti social behaviour initiatives etc). BCC will ensure that suitable guarantees regarding security and appropriate data handling are applied and documented as part of a written agreement.
- When internal BCC departments need to share personal data between each other for a variety of lawful Council reasons.

**Data-processors**
BCC will only engage organisations to act as a Data Processor who meet strict information governance standards. BCC will ensure that suitable guarantees regarding security and appropriate data handling are applied and documented as part of a written agreement.

A Data Processor will process personal data on behalf of BCC **but will not exercise responsibility** for or control over it. Data Processors will have limited responsibilities under the Data Protection Act and these address the necessity to keep personal data secure from unauthorised access, disclosure, destruction or accidental loss.

BCC as the Data Controller **will remain responsible** for the personal data held by a Data Processor and for ensuring compliance with the provisions of the Data Protection Act.

## 10. Training

All staff will be made aware of their obligations to comply with the Data Protection Act 1998 through a rolling programme of awareness training by the staff from the Information Governance Unit and will receive e-learning refresher training every year.

All new full-time and temporary staff, including agency workers, will be provided with training as part of their induction training.

RLOs and DMs, nominated by each department, will receive enhanced Data Protection training from the Information Governance Unit. The content of this training will focus on the role they perform.

DPA awareness training is mandatory for all staff and attendance recorded by Corporate H.R.

## 11. Policy Compliance and Audit

As previously mentioned, the Information Commissioner has wide powers of enforcement. A breach of the act can result fine of up to **£500,000 for the council** and staff should also be aware that in some circumstances, **unlawful access, misuse or being reckless** in the handling of personal data may constitute a **criminal offence**.

The Information Governance Unit will examine, by way of Data Protection compliance audits, personal data processed on electronic and manual information systems. The overriding purpose of an audit is to ensure that information processed is gathered, retained, used and disclosed in accordance with the Data Protection Act 1998. This will be in addition to any internal departmental checks and monitoring.

## 12. Equality Impact Assessment

The Data Protection Act 1998 provides legal rights to all individuals and there are no equality issues to be addressed regarding the issue of this policy

## 13. Policy Monitoring and Review

This policy will be reviewed annually by the Information Governance Unit, or as appropriate and in response to changes to legislation, council policies, technology, increased risks and new vulnerabilities or in response to security incidents.

## 14. Freedom of Information

The content of this policy in Sections 1 to 15 is suitable for public disclosure as part of BCC publication scheme under the Freedom of Information Act 2000. The accompanying appendices listed at 1 to 5 are for internal use only.

## 15. Appendices – Data Protection Procedures

| Appendix | Procedures |
|---|---|
| 1 | How to deal with a request from an individual for their personal data (referred to as a 'subject access request') |
| 2 | Data Subjects Rights regarding the processing of personal data |
| 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 |
| 4 | How to set up a data processing agreement with a third party who will process data on behalf of the council |
| 5 | How to handle a significant data breach |