Causeway Coast & Glens Borough Council

DATA PROTECTION POLICY

Policy Number	CCG/5/14/CS
Version Number	1
Author	P McLaughlin
Date	29.10.14

Date of Screening of Policy	30.10.14
EQIA Recommended?	NO
Date Adopted by Council	27.11.14
Date Policy Revised	14.5.18

INDEX

DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Data Protection legislation places a range of legal obligations on persons who record and process personal information relating to living individuals. Although this area of the law appears to be complicated, the legislation simply requires that adequate controls exist to protect individuals from the consequences of poor quality information and/or the misuse of information held about them.

1.2 The legislation does not affect the Council when using information which does not directly or indirectly identify an individual. Additionally, the legislation does not apply in circumstances when the Council is simply giving advice in general terms, for example Council byelaws or matters of Council policy.

1.3 The term 'processing' includes any function that can be performed using information and includes the actual disclosure of information. The Council has introduced this Data Protection Policy for the information of all Elected Members, Council employees and Council residents.

1.4 The Data Protection Policy constitutes the framework document to guide the Council's practice in relation to meeting its requirements under Data Protection legislation.

2. POLICY STATEMENT

2.1 It is the intention of Causeway Coast and Glens Borough Council to fulfil its legal obligations within the provisions of Data Protection legislation. The Council will ensure that the Information Commissioners Office is properly when and where required.

2.2 Individuals whose personal information is held and processed by the Council can be assured that their information will be processed in accordance with the eight Data Protection Principles (Appendix 1).

2.3 It is the aim of the Council to ensure that all appropriate staff are properly trained, kept fully informed of their obligations under Data Protection legislation and that they are aware of their personal data protection liabilities. Any Council employee deliberately acting outside their recognised responsibilities may be subject to the Council's disciplinary procedures.

2.4 It is the intention of the Council to allocate such resources as may be required to ensure the effective operation of the Data Protection Policy.

Signed: _____ Date: _____

Mayor
Causeway Coast and Glens Borough Council

Signed: _____ Date: _____

Chief Executive
Causeway Coast and Glens Borough Council

3. ACCOUNTABILITY AND RESPONSIBILITIES

The Chief Executive has overall responsibility for the administration and implementation of the Council's Data Protection Policy. Each Director and Head of Service will assume authority for the compliance of staff within their directorate and service area.

4. GUIDING PRINCIPLES

4.1 Fair Obtaining and Processing

Causeway Coast and Glens Borough Council will ensure that as far as practicable, all individuals whose details are processed by the Council are aware of the way in which that information will be obtained, held and disclosed. Whenever possible, individuals will be informed of the potential recipients of the information. Processing personal information by the Council will be fair and lawful, and, in addition, it is Council policy that individuals will not be misled as to the purpose to which Council will process the information.

4.2 Information Quality and Integrity

The Council will endeavour to process personal information which is accurate, current and is of good quality. Information, which is obtained by the Council, will be adequate and not excessive for the purpose for which it is processed. In addition, information will be kept by the Council for no longer than is necessary for the purposes for which it was obtained.

4.3 Subject Access

The Council will respond positively to subject access requests, replying as quickly as possible, and in any event within the one calendar month time limit. Whilst individuals have a general right of access to any of their own personal information which is held, the Council will be mindful of those circumstances where an exemption may apply.

4.4 Technical and Organisational Security

The Council has in place appropriate security measures as required by Data Protection legislation. Information systems are installed with adequate security controls and Council employees who use these systems will be properly authorised to use them for Council business. In addition, Council employees will be kept fully informed about overall information security procedures and the importance of their role within these procedures.

Similarly, manual filing systems are held in secure locations and they are accessed only by authorised Council staff.

5. EVALUATION AND REVIEW OF THE POLICY

5.1 The Data Protection Policy, will under normal circumstances, be managed and reviewed annually. The reviews to the policy will be subject to scrutiny and from time to time updates and re-issues will be circulated.

5.2 The policy will be reviewed sooner in the event of any one or more of the following:

a) Weakness in the policy is highlighted;
b) Weakness in hardware and software controls are identified;
c) In case of new threat(s) or changed risks;
d) Changes in legislative requirements;
e) Changes in Government or other directives and requirements.

6. SECTION 75 EQUALITY AND GOOD RELATIONS

Causeway Coast and Glens Council is fully committed to meeting its obligations in relation to Equality and Good Relations under Section 75 of the Northern Ireland Act. In this regard this policy will be screened using Section 75 guidelines and will be subject to an Equality Impact Assessment if found necessary as a result of the screening process.

7. CONTACT DETAILS

Any issues or queries relating to this policy should be addressed to:

Head of Policy and Community Planning
Causeway Coast and Glens Borough Council

Tel: 028 777 60318
E-Mail: elizabeth.beattie@causewaycoastandglens.gov.uk

APPENDIX 1

THE DATA PROTECTION PRINCIPLES

The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either— (a) the data subject has given consent to the processing for that purpose, or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where— (a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and (b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 40).

(5) The second case is where— (a) the processing is strictly necessary for the law enforcement purpose, (b) the processing meets at least one of the conditions in Schedule 8, and (c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 40).

(6) The Secretary of State may by regulations amend Schedule 8 by adding, varying or omitting conditions.

(7) Regulations under subsection (6) are subject to the affirmative resolution procedure.

(8) In this section, “sensitive processing” means— (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; (c) the processing of data concerning health; (d) the processing of data concerning an individual’s sex life or sexual orientation

The second data protection principle

(1) The second data protection principle is that— (a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that— (a) the controller is authorised by law to process the data for the other purpose, and (b) the processing is necessary and proportionate to that other purpose.

(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

The third data protection principle.

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The fourth data protection principle

(1) The fourth data protection principle is that— (a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and (b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as— (a) persons suspected of having committed or being about to commit a criminal offence; (b) persons convicted of a criminal offence; (c) persons who are or may be victims of a criminal offence; (d) witnesses or other persons with information about offences.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose— (a) the quality of personal data must be verified before it is transmitted or made available, (b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and (c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.
(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).