www.calderdale.gov.uk

DATA PROTECTION POLICY

Author	Tracie Robinson – *DPO, Corporate Information Manager, SIRO*
Status	Approved originally on 15/09/16
Reviewed and approved by	Information Governance/ICT Managers Team
GDPR date	25th May 2018
Approved Reviewers	Tracie Robinson/Rob McNally
Date of Issue	22nd June 2017
Date of Next Review	22nd June 2019
Service	Information Governance

DATA PROTECTION POLICY

1. Introduction

The Data Protection Act 1998 came into force on 1 March 2000 and superseded the Data Protection Act 1984. The General Data Protection Regulations (GDPR) have made some advancements in the rights of individuals and how organisations can handle their data. The purpose of the legislation is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their explicit consent wherever possible. The Act covers personal data relating to living individuals, and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data. Calderdale Council is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1.1 Calderdale Metropolitan Borough Council (The Council) intends to fulfil its obligations under the Data Protection Act 1998 (The Act) and the GDPR.

1.2 The Council is required to maintain certain personal data about the citizens of Calderdale in order to satisfy our operational and legal obligations and to fulfil our Corporate Priorities.

1.3 This policy outlines the responsibilities of all employees, contractors and elected Members of Calderdale Council and the Rights of Data Subjects.

2. Scope of the Policy

2.1 The Data Protection Act and GDPR applies to electronic and paper records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

2.2 The Council collects a large amount of personal data every year including: staff records; names and addresses of members of the public; databases; references; benefits details and fee collection as well as the many other different types of information used by the Council.

3. Specific Measures

All Directorates will:

- Ensure that all relevant staff attend/complete any offered training on data protection;
- Inform the Information Governance Team of any new services, projects and processes involving the use of personal data, or of significant changes to existing ones so that a Privacy Impact Assessment can be carried out;

- Report all losses, thefts or breaches of security involving personal data to the Information Governance Team;
- Notify the Information Governance Team of all existing or intended information sharing agreements or protocols; and
- Participate in Data Protection audits.

4. Responsibilities

4.1 Data Protection means that the Council must:

- Manage and process personal data properly;
- Protect the individual's rights to privacy;
- Provide an individual with access to all personal information held on them.

4.2 The Council has a legal responsibility to comply with the Act and has overall responsibility for this policy. The Council, as a public body, is named as the Data Controller under the Act.

4.3 The Council is required to notify the Information Commissioner of the processing of personal data; this is included in a public register. The public register of data controllers is available on the Information Commissioner's website. Details of the Council's registration can be sought from the Information Governance Team.

4.4 The Council's Corporate Information Governance Team is responsible for drawing up guidance on good data protection practice and promoting compliance with this guidance through advising staff on the creation, maintenance, storage and retention of their records which contain personal information.

4.5 Every member of staff that holds information about identifiable living individuals has to comply with data protection in managing that information. Individuals can be liable for breaches of the Act.

4.6 The Council's Data Protection Officer is Tracie Robinson (Legal Services) who can be contacted at information_management@calderdale.gov.uk.

5. Notification

5.1 The Council will ensure that we notify our purposes for processing personal data with the Information Commissioner, as is our duty under s19 of the Act.

5.2 Any new purposes for processing will be notified as soon as possible and will not be carried out without the explicit consent of the Data Subject (unless required by law).

6. Principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and Calderdale Council's policies and procedures are designed to ensure compliance with them.

6.1 **Personal data must be processed lawfully, fairly and transparently.**

Calderdale Council's Privacy Notice Procedure is set out in the Information Governance Intranet pages along with guidance on all topics relating to ICT and information management.

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

6.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;

6.1.2 the contact details of the **Data Protection Officer**, where applicable;

6.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

6.1.4 the period for which the personal data will be stored;

6.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing;

6.1.6 the categories of personal data concerned;

6.1.7 the recipients or categories of recipients of the personal data, where applicable;

6.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

6.1.9 any further information necessary to guarantee fair processing.

6.2 **Personal data can only be collected for specified, explicit and legitimate purposes.**

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Calderdale Council's registration.

6.3 **Personal data must be adequate, relevant and limited to what is necessary for processing.**

6.3.1 The Data Protection Officer is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

6.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer.

6.3.3 The Data Protection Officer will ensure that, on an annual basis, all data collection methods for electronic systems are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

6.3.4 If data is given or obtained that is excessive or not specifically required by the Council's documented procedures, the Data Protection Officer is responsible for ensuring that it is securely deleted or destroyed.

6.4 **Personal data must be accurate and kept up to date**

6.4.1 Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

6.4.2 It is also the responsibility of individuals to ensure that data held by the Council is accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate at the date of submission.

6.4.3 Employees/Staff/Customers/service users should notify Calderdale Council of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is noted and acted upon.

6.4.4 The Data Protection Officer/system owner is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

6.4.5 On at least an annual basis, the Data Protection Officer/System Owner will review all the personal data maintained by the Council systems, by reference to the Information Asset Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed.

6.4.6 The Data Protection Officer/System Owner is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, the information that is inaccurate and/or out-of-date is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

6.5 **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing**

6.5.1 Where personal data is retained beyond the processing date, it will be (minimised/ encrypted/pseudonymised) in order to protect the identity of the data subject in the event of a data breach.

6.5.2 Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

6.5.3 The Data Protection Officer/Corporate Records Officer must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

6.6 **Personal data must be processed in a manner that ensures its security**

6.7 **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental lost or destruction of, or damage to, personal data.**

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

6.8 **Personal data shall not be transferred to a country or territory outside the European Union 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**

The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

6.8.1 ***Safeguards***

An assessment of the adequacy by the data controller taking into account the following factors:

- The nature of the information being transferred;
- The country or territory of the origin, and final destination, of the information;
- How the information will be used and for how long;
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- The security measures that are to be taken as regards the data in the overseas location. (This is a UK-specific option.)

6.8.2 ***Exceptions***

In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country, or an international organisation, shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

- the transfer is necessary for important reasons of the public interest;

- the transfer is necessary for the establishment, exercise or defence of legal claims;

- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

- the transfer is made from a register which, according to Union or Member State law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

  A list of countries that satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.*

6.9 **Accountability**

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform PIAs (Privacy Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

7. Conditions for Processing

7.1 The Council must only process personal data if one of the requirements in Schedule 2 of the Act is met.

These requirements are that:

7.1.1 The individual has given his or her consent to the processing.

7.1.2 The processing is necessary for the performance of a contract with the individual.

7.1.3 The processing is required under a legal obligation.

7.1.4 The processing is necessary to protect the vital interests of the individual.

7.1.5 The processing is necessary to carry out public functions.

7.1.6 The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

7.2 The Council must only process sensitive personal data if one of the requirements in Schedule 2 of the Act is also met.

These requirements are that:

7.2.1 The individual has given his or her explicit consent to the processing.

7.2.2 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

7.2.3 The processing is necessary to protect the vital interests of the individual.

7.2.4 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

7.3 The Council will aim to ensure that all employees, contractors and elected Members are trained and aware of their obligations under the Act.

7.4 If an employee breaches the Act they will be subject to internal disciplinary procedures.

8. Rights of Data Subjects

8.1 Individuals have a right of access to personal information held by the Council about them. The legislation calls this a Subject Access Request. This means that members of the public and employees have a right to see information the Council holds about them.

8.2 The Council will respond to requests of access to personal data in accordance with the Act and our subject access procedure.

8.3 The Council will aim to respond to all requests from individuals for access to their personal data within the timescale set out in the Act. We will respond to such requests when they are received in writing with an adequate description to identify the location of the data requested.

8.4 The Council will not charge for Subject Access Requests.

8.5 The Act allows exemptions from subject access and non-disclosure of information in specific and limited circumstances. The exemptions relate to:

- National security.
- Crime and Taxation.
- Some areas of Health, Education and Social Work.
- Regulatory activity.
- Journalism, literature and art.
- Disclosures required by law or made in connection with legal proceedings.

8.6 Individuals have a right to write to the Council at any time to request that the processing of their personal data ceases. The Council will endeavour to comply with such requests and cease processing where practicable.

- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another

controller.

- The right to object to any automated profiling without consent.

8.7 Data subjects may make data access requests called Subject Access Requests. This procedure also describes how Calderdale Council will ensure that its response to the data access request complies with the requirements of the Regulation.

8.8 **Complaints**

Data Subjects who wish to complain to Calderdale Council about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer by means of an email to information_management@calderdale.gov.uk.

Data Subjects may also complain directly to the ICO and Data Protection Officer.

Where Data Subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint with the Data Protection Officer.

9. Information Sharing

9.1 Information sharing with external agencies will be carried out under a written agreement (*see Information Sharing Protocol*) setting out the scope and limits of sharing, and the safeguards to be put in place. Any disclosure of personal data will be in compliance with approved procedures.

10. Associated Policies

10.1 This policy has been formulated within the context of the following Council documents:

- Records Management Policy.
- Personal Information Management System (PIMS).
- Subject Access Request Procedure and Form.
- Information Security Policy.
- Freedom of Information Policy.
- Information Sharing Protocol.

10.2 Compliance with this policy will in turn facilitate compliance not only with the Freedom of Information Act 2000, but also with other legislation and regulations (including audit, information sharing and equal opportunities affecting the Council).

11. Guidance

11.1 Guidance on the procedures necessary to comply with this policy is available from the Corporate Information Manager. This guidance covers:

- Introduction to Data Protection, including Data Protection Principles, types of data involved and key concepts.
- Best practice guidelines.
- Procedures for dealing with Subject Access Requests.
- Who to contact for assistance.
- Application Form.

11.2 This guidance is also available on the Intranet.

Status

This policy was approved by the Information Governance/ICT Managers Group on 15/09/2016. It will be reviewed every two years.

Contacts

Information Governance Team

Information_management@calderdale.gov.uk

Document Owner and Approval

The system owner/team manager is responsible for ensuring that this procedure is complied with.

A current version of this document is available on the Information Governance intranet pages.

Signature: Date: 22nd June 2017

Change History Record

DATA PROTECTION POLICY

Issue	Description of Change	Approval	Date of Issue
1	Initial Issue	Corporate Information Manager/DPO/SIRO	15/09/2016
	Posted on intranet		22/06/2017