London Borough of Redbridge

Data Protection Policy

Ambitious for Redbridge

Classification: Not Protectively Marked
Date: November 2017 Version: 3.0
Owner(s): Information Governance Board

Change Control

This document is subject to change control and amendments will be recorded below whilst the document is in draft. Pre-release versions should have the extension 0.10, 0.20 and so on.

Version	Date reviewed	Summary of Changes	Updated by	Approved by	Date published	Published to
0.1	22/01/13	Initial draft	Tim Rodgers, Information Governance Manager	Approved by 1GB OG to go to 1GB	Not published	N/A
0.11	13/02/13	1GB draft	Tim Rodgers, Information Governance Manager			
0.12	11/03/13	Post 1GB draft	Tim Rodgers			
1.0	13/03/13	Publication Draft	Tim Rodgers	Information Governance Board 13/3/13	15/3/13	Intranet
1.1	12/10/2016	Review and Update. Updated logo	Aysha Mukhtar			
1.2	18/10/2016	Reordered 1GB Draft	Lesley Holmes			
2.0	25/10/2016			Information Governance Board		
2.1	14/11/2017	GDPR compliance	Shane Murphy			
3.0	16/11/2017	GDPR minor amendments	Aysha Mukhtar	Information Governance Board 19/1/18	07/02/18	Intranet

For details of previous amendments, see previous versions of the document.

This policy will be reviewed within six months of its initial publication and at least annually thereafter or whenever legal or statutory changes demand. The review body will be the Information Governance Board.

Contents

1 Introduction

The General Data Protection Regulation (GDPR) and the Data Protection Act 1998 (DPA 1998) places an obligation on the Council, as the data controller to put safeguards in place to ensure that the Council collects, handles, processes, stores and uses personal information **fairly, lawfully** and **securely** by complying with the various principles set out in the GDPR and in the DPA.

This policy outlines how the Council will comply with its new responsibilities under the GDPR that build upon those already established by the DPA. The UK Government is in the process of replacing the DPA with new successor legislation based upon the requirements of the GDPR

2 Statement

The Council is committed to ensuring that it protects the rights and freedoms of all individuals with respect to the personal data it holds about them, whether in their personal or family life, business or professional capacity.

We, therefore, fully endorse and adhere to the new standards and improved principles set out in the GDPR that build upon the DPA principles (Please see Appendix 1). The GDPR Principles are provided in section 4 below.

3 Scope

This policy applies to all employees, council members, contractors, third party employees, agency workers, temporary staff, and partner organisation staff. It also includes schoolbased staff where the Board of Governors has adopted the policy.

This policy applies to all users who handle information belonging to the Council regardless of their work location i.e. in the office, at home, remote or mobile working and applies to all personal data collected, handled, stored, transmitted or shared. It therefore includes information held electronically, on paper, or other physical media which is shared

electronically, physically, orally or visually e.g. email, on paper, in a photograph, by telephone, presentation and/or video conferencing, etc.. (This list is not exhaustive).

This includes information relating to current, past and prospective employees, suppliers, residents, service users, and others with whom it may come in contact with.

4 Definition of Personal Data and Special Categories of Data

The Council is committed to achieving compliance with the GDPR. The GDPR provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "special categories" of personal data.**

Personal data means any information relating to an identified or identifiable natural person who may be identified from any of the following:

- Name, an identification number, location data, an online identifier (e.g. cookies); or
- To one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of data are defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Genetic and biometric data.

The GDPR principles and the Council's role in meeting the principles These

principles require that personal data shall be:

1. processed fairly, lawfully and in a transparent manner in relation to the data subject, in particular, shall not be processed unless specific conditions are met;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interst, scientific or historical research purposes are compatible with the original purpose, subject to further conditions (Article 89(1).;

3. adequate, relevant and limited to what is necessary for the purpose for which they are processed (minimum necessary dataset);

4. accurate and, where necessary, kept up to date; personal data that are inaccurate must be erased or rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary; archiving in the public interest for historical research, and statistical purposes is permitted so long as the appropriate technical and organisational controls are in place to safeguard the rights and freedoms of data subjects;

6. processed in a manner that ensure appropriate security of the personal data including protection against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data using appropriate technical and organisational measures;

Therefore, the Council will aim to ensure that the GDPR lawful conditions for processing are met by ensuring one of the following applies:

a. the data subject has provided consent for the processing of personal data for one or more specific purposes;

b. processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with a legal obligation to which the Council is subject;

d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e. Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the Council;

f. Processing is necessary for the purpose of the legitimate interests of the Council or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The Council will ensure that the following practical measures are deployed, where appropriate, to ensure and demonstrate GDPR compliance:

1. inform people why we are processing their data, who we will share their data with through our various Privacy Notices and Fair Processing Notices and other means available;

2. ensure that all staff and people working for and with the Council have completed Data Protection training as part of their induction and that this is refreshed annually;

3. ensure that all contractors and agents are fully aware of the standard of data protection compliance required and ensure that their procedures are adequate to safeguard any personal data processed on the Council's behalf.

4. ensure that appropriate clauses are included within contracts of employment and for services provided

5. ensure that the rights of people about whom information is held can be fully exercised under the GDPR and any successor legislation.

6. hold only the minimum personal data necessary to carry out the Council's functions, make every effort to ensure the accuracy of the information held and ensure that where records include opinions and/or intentions, that these are carefully and professionally expressed

7. where it is appropriate to share information the Council will ensure that people are informed that this will happen and appropriate arrangements, including model contractual clauses, information sharing agreements and protocols are in place for regular sharing of personal information e.g. for providing care and liaising with the Health Service

8. ensure that data which is no longer required is securely destroyed and that data of historical importance and/or of value for future research or statistical purposes is identified and archived according to the Council's Retention Schedule and Data Disposal Procedure.

9. ensure data protection by design and operational implementation through project management methodology and to periodically review existing security measures and access in order be effective in preventing the unauthorised or unlawful processing, breach, alteration, damage or destruction of data. Keep records of data

processing activities with their legal justification and data retention periods and map all data flows. The security measures will be applied in accordance with the CouncWs Information Security Policy.

10. A Privacy Impact Assessment (PIA) will be completed when new projects or processing operations are likely to result in a high risk to the rights and freedoms of natural persons by the processing of personal data. The PIA shall be maintained for the duration of that processing activity.

11. only transfer data to a country or territory outside the European Economic Area (EEA) recognised as having an adequate level of protection for the rights and freedoms of data subjects in accordance with the Information Commission published guidance and through appropriate Privacy Notices inform data subjects of the security measures to protect the transfer of data outside of the EEA

12. ensure all subject access requests from individuals to access their personal data are dealt with as quickly as possible and within the 30 day time scale required in the GDPR, subject to the data subject meeting the requirements set out in the GDPR

5 Reporting breach of the GDPR, DPA or Information Security Incidents

Any Council employee, contractor or elected member who suspects that a personal data breach of the GDPR or an Information Security Incident has or will occur, **must** report any such breach or incident or any concerns about information security at the earliest opportunity to the service desk through the Information Security Incident Reporting Procedure available on the intranet.

A personal data breach, must be reported to the Information Commissioner's Office (ICO) not later than 72 hours after discovery. This reporting responsibility to the ICO currently rests with the SIRO, Caldicott Guardian, and Information Governance Manager.

If it is not appropriate to use the Information Security Incident Reporting Procedure then breaches should be escalated by:

- Contacting the appropriate Head of Department; or by contacting the Councils Data Protection Officer, or Head of Audit under the Council's Whistleblowing Policy.

- Council Members must report breaches of information security to the Head of Legal and Constitutional Services

The incident will be investigated in accordance with the Information Security Incident Reporting Procedure. Given the legal responsibility identified above the SIRO, Caldicott Guardian and the Information Governance Manager must be kept appraised of developments from the earliest opportunity.

6 Responsibilities

Responsible	Senior Information Risk Owner (SIRO) The SIRO is responsible for ensuring organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist.
Accountable	The Chief Executive has ultimate accountability and authority for the policy.
Conscience	The Caldicott Guardian is the "conscience" of the Council, providing a focal point for service user and patient information sharing issues and advising on the options for lawful and ethical processing of information as required, within the People Directorate.
Consulted	Information Governance Board - It is the responsibility of the Information Governance Board to ensure that: • This policy is well publicised, updated and remains relevant; • If users cannot access the intranet, provision is made to distribute the policy and any updates through their appropriate reporting structure; and • Users are able to meet the obligations and responsibilities set out in this policy.
Members	Members should understand and apply the policy in their day-to-day activities; • Are aware of any changes to the policy; and • Understand how to report breaches as set out in sections below
Information Risk Management	Information Asset Owners (IAO) and Information Asset Managers (1AM) IAOs and IAMs are responsible for understanding and addressing risks to personal data/information assets they "own" and provide assurance to the SIRO on the security and use of these assets.

Operational	Managers have basic responsibility for the manner in which personal data is used or processed within their department or areas of responsibility and must liaise with the Information Governance Manager in all aspects of data protection. It is a manager's responsibility to have a good working knowledge of Information security and the GDPR and the relevant Codes of Practice. Managers should also ensure that their staff are aware of the Data Protection policy and the GDPR and any successor legislation. All Council employees, agency workers, contractors and consultants, staff members of partner organisations (who have been permitted access to the Council's information- Understand and apply the policy in their day-to-day activities;

	• Are aware of any changes to the policy; and • Understand how to report breaches as set out in sections below.
Communicated	Via the Intranet, staff newsletter, training, briefings

7 Policy Non Compliance

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in an inability to provide necessary services to the public, a huge fine from the Information Commissioners Office, enforcement action taken against the Council or individuals and reputational damage to the Council.

Users found to be in breach of this policy (e.g. recklessly handling personal data) may be subject to the Council's disciplinary procedures, which may lead to dismissal. If a criminal offence has been committed, further action will be taken to assist in the prosecution of users involved.

8 Policy Awareness

A lack of awareness of a new or updated policy cannot be used to defend liability in the event of an information security breach. This policy takes precedence over any local procedures.

This Policy will be periodically communicated to staff using the MetaCompliance online policy acceptance system, and be available on both the intranet and Redbridgei.

9 Criminal offences

The UK is able to implement legislation to impose criminal penalties for infringement of the GDPR, the Council will assist the relevant authorities in the prosecution of these as appropriate. Details of the offences can be found on the ICO website

Anyone found guilty of a criminal offence could face an unlimited fine in the Magistrate's Court or an unlimited fine in the Crown Court.

10 Complaints made under the GDPR

Complaints regarding the handling of requests for information under the GDPR and any successor legislation shall be dealt as per the CouncWs Corporate Complaints Procedure.

11 Related Policies & Legislation

This policy should be read in conjunction with:

- Information Security Policy Framework
- Information Security Incident Reporting Procedure
- General Data Protection Regulation
- Data Protection Act 1998 and any UK successor legislation

Appendix 1 - Data Protection Act Principles 1998 (applicable until the enactment of successor legislation)

The eight data protection principles and the Council's role in meeting the principles

These principles require that personal data:

1) shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

2) shall be 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 in relation to the purpose or purposes for which they are processed;

4) shall be accurate and, where necessary, kept up to date;

5) shall not be kept for longer than is necessary;

6) shall be processed in accordance with the rights of data subjects under the DPA 1998;

7) appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

8) shall not be transferred to a country or territory outside the European Economic Area 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.

Therefore, the Council will aim to ensure that we:

a) follow best practice in all personal data processing

b) follow the relevant conditions for the fair and lawful processing of personal data (set out in DPA Schedule 2) and for processing sensitive personal data (set out in DPA Schedule 3)

c) tell people why we are processing their data, who we will share their data with through our Fair Processing Notice and other means available.

d) where possible obtain consent from the person whose data we are processing

e) ensure that all staff and people working for and with the Council have completed Data Protection training as part of their induction and this is refreshed annually

f) ensure that all contractors and agents are fully aware of the standard of data protection compliance required and ensure that their procedures are adequate to safeguard any personal data processed on the Council's behalf.

g) ensure that appropriate clauses are included within contracts of employment and for services provided

h) ensure that the rights of people about whom information is held can be fully exercised under the DPA 1998.

i) hold only the minimum personal data necessary to carry out the Council's functions, make every effort to ensure the accuracy of the information held and ensure that where records include opinions and/or intentions, that these are carefully and professionally expressed

j) where it is appropriate to share information the Council will ensure that people are informed that this will happen and appropriate arrangements, including information sharing agreements and protocols are in place for regular sharing of personal information e.g. for providing care and liaising with the Health Service

k) ensure that data which is no longer required is securely destroyed and that data of historical importance and/or of value for future research or statistical purposes is identified and archived according to the Council's Retention Schedule and Data Disposal Procedure.

l) periodically review existing security measures and access in order be effective in preventing the unauthorised or unlawful processing, breach, alteration, damage or destruction of data. The security measures will be applied in accordance with the Council's Information Security Policy.

m) A Privacy Impact Assessment will be completed when new projects dealing with the processing of personal data are initiated and these shall be maintained for the duration of that processing activity.

n) only transfer data to a country or territory outside the European Economic Area recognised as having an adequate level of protection for the rights and freedoms of data subjects in accordance with the Information Commission published guidance.

o) ensure all subject access requests from individuals to access their personal data are dealt with as quickly as possible and within the 40 day time scale allowed in the DPA, subject to the data subject meeting the requirements set out in the DPA