General Data Protection Regulation (GDPR) Policy

If printed, copied, or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

www.lbbd.gov.uk

Document Control

Title	General Data Protection Regulation Policy
Document Type	Approved
Author	Information Governance Manager/DPO
Owner	SIRO
Subject	General Data Protection Regulation
Government Security Classification	Official
Created	March 2018
Approved by	Assurance Group
Date Approved	20 April 2018
Review Date	May 2019 or earlier where there is a change in the applicable law or a Council restructure affecting this Policy Guidance

Version Control

Version	Date	Author	Description of Change
1	1/02/17	Yvonne Mason, Information Governance Manager	New Policy Draft
1.1	13/04/17	Yvonne Mason, Information Governance Manager	Addition of reference to Caldicott Guardian S4
2	13/04/17	Yvonne Mason, Information Governance Manager	Approval by Assurance Group
3	11/03/18	Yvonne Mason Information Governance Manager/DPO	Annual renewal revised to include GDPR all references to the DPA have been replaced. Section 1,3,4 and 7

1. Introduction

The London Borough of Barking and Dagenham ('the council') is fully committed to compliance with the requirements of the General Data Protection Regulation 2016/279 ('the Act'). The council will therefore, follow procedures which aim to ensure that all employees, elected Members, contractors, consultants, partners or other servants or agents of the council (collectively known as data users) who have access to any personal data held by or on behalf of the council are fully aware of and abide by their duties under the General Data Protection Regulation.

The processing of personal data is essential to many of the services and functions carried out by local authorities. The council recognises that compliance with the Act will ensure that processing is carried out fairly, lawfully and transparently.

The GDPR, and Article 8 of the Human Rights Act 1998, both stress that the processing of personal data needs to strike a balance between the needs of the organisation to function effectively and efficiently and respect for the rights and freedoms of the individual. This policy sets out how the council intends to safeguard those rights and freedoms.

Obligations and responsibilities under the General Data Protection Regulations are not optional; **they are mandatory**. There can be harsh penalties, up to €20 million or 4% of global turnover for the preceding year (whichever is the greater) in relation to breaches of rights and obligations and up to €10 million or 2% of global turnover for the preceding year (whichever is the greater) imposed for non-compliance regarding Control and Mitigation.

The council will therefore, follow procedures that aim to ensure that all staff, elected members, contractors, agents, consultants, partners, or any other person working for the council who have access to any personal data held by or on behalf of the council is fully aware of, and abides by their duties and responsibilities under the Act.

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken.

As well as the council, any individual who knowingly or recklessly processes data without appropriate consent or proper authorisation, for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to the council's disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution and possible criminal conviction under the Criminal Justice and Immigration Act 2008.

2. Scope

This policy applies to the collection and processing of all personal data held by the council, falling within the scope of the Act, in all formats including paper, electronic, audio and visual. It applies to all employees of the council.

3. Personal and Special Category Personal Data

The Act provides conditions for the collection and processing of any personal data. It also makes a distinction between **personal data and 'special category' personal data**.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category personal data is 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 or sexual orientation;
- genetics
- biometric data (where used for ID purposes)

Although there are clear distinctions between personal and special category data for the purposes of this policy the term *'personal data'* refers equally to *'special category data'* unless otherwise stated.

The GDPR rules for special category data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

4. Personal Data processed by the council

The council processes personal data for many reasons including in relation to the services it provides and as an employer. A description of the types of personal data processed and the purposes for processing are included in the Council's Data Protection Registration entry which is publicly available on the website of the Information Commissioner's Office ('The ICO').

This personal data must be handled and dealt with in accordance with the Act and this policy. There are safeguards within the Act to ensure personal information is collected, recorded and used whether it is on paper, computer records or recorded by any other means.

The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes personal data. This includes those who work at/from home or have remote or flexible patterns of working.

Directors, Service Heads and Managers have immediate responsibility and accountability for data protection matters in their own areas of work including:

- development, implementation, and review of departmental Data Protection Procedures that support this policy.
- ensuring compliance with Information Governance policies and standards established by the council and their service.
- ensuring that new information systems in their work area are designed to comply with this policy (tested against the Privacy Impact Assessment toolkit).
- notifying the Data Protection Officer of the development of any new systems in their area of work that utilise personal data.

Caldicott Guardian is responsible for the safeguarding of information processed for social care work and will oversee all procedures for protecting the confidentiality of service user information and enabling the appropriate information sharing. The Caldicott Guardian will ensure that compliance with this policy is achieved and will work proactively (supported by nominated staff) to ensure that personal data processed for social care is appropriately safeguarded to meet the requirements of the GDPR, and other relevant legislation.

The Caldicott Guardian will provide advice, guidance, and expertise to the Assurance Group in relation to social care service user information and will support the Information Governance structures in place within the council.

Staff and Elected Members (including consultants, contractors, temporary, part time and agency staff) will have immediate responsibility to;

- work in a manner which will ensure the security and good management of all personal information they have access to, and
- proactively alert management to suspected poor data protection practices

The Principles of Data Protection

Anyone processing personal data must comply with 6 principles of good practice. These principles are legally enforceable and can be summarised as follows:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. In accordance with the rights of data subjects under the Act

5. Fair Processing

In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as is necessary to ensure that they are likely to understand: -

a) The purposes for which their personal data are to be processed;
b) The likely consequences of such processing and;
c) Whether particular disclosures can be reasonably envisaged

6. Notification

The national body for the supervision of GDPR is the Information Commissioners' Office to whom the Chief Executive notifies his/her purposes for processing personal data.

This notification process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the GDPR that the public should know or be able to find out who is carrying out the processing of personal data and for what purpose.

A copy of the council's notification details is available on the Information Commissioner's website.

www.ico.gov.uk

7. Individuals' Rights

The council recognises that access to personal data held about an individual is a fundamental right provided in the Act. These rights include:-

- The right to be informed
- The right of access to personal information
- The right to request rectification
- The right to request erasure
- The right to restrict processing in certain circumstances
- The right to data portability
- The right to object to processing
- Rights to automated decision making including profiling

This right is called ‘Data Subject Access Request’. The council will ensure that all requests from individuals to access their personal data are dealt with as quickly as possible and within the 30 calendar-day timescale allowed in the legislation, as long as the data subject meets the requirements set out in this policy. To minimise delays and unnecessary work all requests from data subjects must:

- Be made in writing (paper or email) to dpo@lbbd.gov.uk
- Be accompanied by adequate proof of the identity of the data subject and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or, authorised agent).
- Specify clearly and simply the information required.
- Give adequate information to enable the requested data to be located
- Make it clear where the response should be sent.

The Data Protection Officer must be informed of any request to take action against one or more of these rights.

The Act allows exemptions from providing information to individuals making a subject access request, and non-disclosure of information, in specific and limited circumstances. The council will normally apply the exemptions and the non-disclosure of information rules, unless it is satisfied that it is appropriate or reasonable not to do so and, in any event, will always do so in circumstances where it is deemed necessary to the effective operation of the council, for the prevention and detection of crime, to protect the individual or is required by law.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be dealt with under an appropriate internal complaints procedure, or, in the case of an employee through the council’s grievance process.

Ultimately if a data subject continues to be dissatisfied, she/he has the right to ask the Information Commissioner’s Office (ICO) to carry out an assessment of their case and/or pursue a legal remedy.

8. Legal Requirements

The council may be required to disclose personal data by a court order, or to comply with other legal requirements including prevention or detection of crime, apprehension of an offender or gathering of taxation.

External agencies or companies contracted to undertake processing of personal data on behalf of the council must be required to demonstrate, via a written agreement, that personal information belonging to the council will be handled in compliance with the GDPR and that it has the necessary technical and organisational security measures in place to ensure this.

Any sharing of council-controlled personal data with external partners for the purpose of service provision must comply with all statutory requirements and corporate policies.

Data matching techniques will only be used for specific lawful purposes and comply with any relevant Codes of Practice.

The Council will follow relevant guidance issued by the Government and the ICO for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and employees have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same. The council reserves the right to monitor telephone calls, email and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO.

The legal basis for this policy is the GDPR which provides the legal parameters for the processing of personal data. However, compliance with other legislation, Codes of Practice, policies and guidance also has relevance, such as;-

- The Freedom of Information Act 2000
- The Computer Misuse Ace 1990
- The Crime and Disorder Act 1998
- Human Rights Act 1998

9. Data Security

The council will process personal data in accordance with its Information Security Policy (and other related Policies and Procedures). To ensure the security of personal data, the council has appropriate physical, technical and organisational measures in place. Council employees are required to comply with the Information Security Policy.

The GDPR requires that appropriate technical and organisational measures shall be taken to protect data against:

- Unauthorised access;
- Unauthorised or unlawful processing;
- Accidental loss, destruction, or damage

Appropriate technical and organisational security measures will include:

- using and developing technological solutions to ensure compliance with the data protection principles
- using and developing physical measures to protect Force assets
- ensuring the reliability of any persons who have access to council information
- reporting and investigating security breaches

These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction, or damage.

All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, hand written notes etc, which contain personal data and are no longer required, will be treated as confidential waste, and disposed of securely.

Where processing of council data is to be carried out by a third party on behalf of the council, the Chief Executive must ensure that the third party provides sufficient guarantees in respect of the technical and organisation measures governing the processing to be undertaken.

10. Training

Data Protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the GDPR and the principles could lead to serious problems, and in some cases may result in significant fines or criminal prosecution.

It is the council's policy that all employees including managers are required to complete the applicable training course annually. This includes employees that do not have internet or email access. Line managers will be responsible for ensuring that staff without internet or email access complete the appropriate training course.

In addition to the corporate training, some post-holders are required to undertake further information governance or data protection training where appropriate for a particular role or within a specific service area.

11. Information Sharing

The council actively encourages the use of Information Sharing Agreements between partners. This approach ensures that information is shared legally, responsibly, and appropriately.

All information sharing agreements must be approved and recorded centrally by the Data Protection Officer before they become valid.

12. Privacy Impact Assessment

The council will use a Data Privacy Impact Assessment (DPIA) toolkit to evaluate all new computer systems to help it determine how data protection compliance can be assured. In addition, all existing systems will be subject to periodic assessment.

DPIA toolkits provide a step-by-step approach to evaluate the test proposed, new or existing information systems for compliance with the legislation. The DPIA process helps to identify weaknesses or risks to data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data holding systems.

The Data Protection Officer must be consulted when carrying out a data protection impact assessment.

13. Our commitment to Data Protection

The Senior Information Risk Officer (SIRO) via the Assurance Group will be accountable for ensuring compliance with this policy across the council.

The council will ensure that individuals handling council personal information will be trained to an appropriate level in the use and control of personal data.

The council have implemented a process to ensure all staff handling personal information know when and how to report any actual or suspected data breach(es), and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

The council will monitor and review its processing activities to ensure these are consistent with the principles of the General Data Protection Regulation and will ensure that its notification is kept up-to-date.

The council will ensure that any new or altered processing identifies and assesses the impact on a subject's privacy as a result of any processing of their personal data, and that appropriate Privacy Notices are maintained to inform data-subjects of how their data will be used.

The council will review and supplement this policy to ensure it remains consistent with the Law and any Compliance Advice and Codes of Practice issued from time to time by the ICO.

14. Disciplinary action and criminal offences

It is not just the Data Controller who is criminally liable. All employees of the council can be personally criminally liable.

Personal data is 'de-identified' if it has been processed in such a way that it can no longer be attributed to a specific data subject (e.g. encryption, anonymisation or pseudonymisation). The Bill makes it an offence to 're-identify' such data without the consent of the data controller, or to process personal data which has been unlawfully re-identified by someone else.

It is also an offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal data without the consent of the data controller. It is also an offence to sell, or offer to sell, illegally obtained personal data and this offence is extended under the Bill to include the retention of personal data. Therefore, an innocent recipient of personal data (where, for example, the data was disclosed to them by mistake) will commit an offence by failing to delete or destroy that data. It is the job of the SIRO to ensure that this doesn't happen and those who within the organisation knowingly handle or process such data will also be guilty of a criminal offence.

Preventing disclosure of personal data

The GDPR retains (and extends) the rights of data subjects to access their personal data. Where a data subject makes such a request (e.g. a subject access request or data portability request) and is entitled to receive the information requested, it will be an offence for the data controller (or its employees, officers or persons under its control) to alter, deface, block, erase, destroy or conceal that information with the intention of preventing its disclosure to the data subject.

The maximum penalty would be an unlimited fine.

In non-criminal cases, it's highly likely the Information Commissioner's Office (ICO) will deem the technical and organisational measures not to have been appropriate. If the Data Controller fails to immediately halt the pseudonymisation or anonymisation process the ICO may apply a fine up to €20 million or 4% of annual turnover, whichever is the greater.

15. Non Compliance

The council is required to proactively report significant data breaches to the Information Commissioners' Office within 72 hours. To do this, anyone who suspects or finds that a data breach, data loss or theft has occurred should be reported to the Data Protection Officer immediately.

Types of suspected data breaches include, but are not restricted to:-

- Accidental disclosure of personal data to another person or organisation
- Inappropriate access to or use of personal data
- The theft of personal information, either paper based or electronic
- Accidental loss of personal data
- Information that has not arrived at its destination
- Fraudulent acquisition of personal data (Blaggers)

The Data Protection Officer will investigate the suspected breach. Where appropriate, particularly in respect of theft, the police may also be notified. If the DPO considers it necessary after concluding the investigation a decision will be made as to whether a report shall be submitted to the Information Commissioners' Office within 72 hours.

Where a breach is shown to have originated from a member of staff it will be dealt with in accordance with the council's procedure for dealing with poor performance and misconduct. Managers will need to decide what action is appropriate based on the circumstances and may wish to seek advice from Human Resources, the DPO and if necessary Legal Services, (particularly in the case of criminal offences).

16. Specific Roles and Responsibilities

Data Controller:

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes and manner for which any personal data are, or are to be, processed. The Chief Executive is the Data Controller for the London Borough of Barking and Dagenham Council

The Data Protection Officer (DPO)

This is a mandatory requirement. The role of the DPO includes the responsibility as the Data Protection Officer which is defined in the Act and includes:-

- informing and advising the controller or the processor and employees who carry out processing of their obligations pursuant to the Regulation.
- Monitoring compliance including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
- Co-operating with the ICO
- Acting as the contact point for the ICO on issues relating to processing, including prior consultation referred to in Article 36 of the Regulation and to consult, where appropriate, with regard to any other matter.

- In the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

All Managers/Supervisors:

It is the responsibility of all Managers/Supervisors and staff who have a supervisory role to ensure that their staff operates within the terms of the Act and any associated policy and procedural guidance. This must include regular checks of work to identify training and development needs in this area and to ensure that the quality of the councils information assets is of a high standard.

All Staff

All employees of the council and any other persons using personal information on behalf of the council have an obligation and personal responsibility to ensure that the information they use is collected, maintained and disclosed in accordance with the terms of the Act, council policy and/or procedural guidance when undertaking their duties.

All staff must comply with the Act regarding disclosures and exemptions with guidance contained in operating rules, conventions, policies and procedures for each system or business area.

17. Sources of information and guidance

This policy is supported by training, awareness and additional guidance made available to staff on the intranet.

The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk

The ICO Data Sharing Code of Practice is available at:

https://ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx#

The ICO Subject Access Code of Practice is available at:

http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

18. Policy Review

This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.