THE LONDON BOROUGH
www.bromley.gov.uk

Policy Document

Data Protection and Confidentiality Policy

January 2020

Document Control

Organisation	London Borough of Bromley
Title	Data Protection and Confidentiality Policy
Author	Lucinda Bowen
File Name	Data Protection and Confidentiality Policy
Owner	Lucinda Bowen
Subject	Information Governance
Protective marking	Not Protected
Review Date	12/12/2019

Revision History

Revision Date	Reviser	Version	Description of Revision
01/01/2018	Lucinda Bowen	1.0	Published version
22/05/2018	DPO	1.1	Published version
12/12/2019	IM Team	1.2	Annual review
21/01/2020	Lucinda Bowen	1.3	Updates and revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
SIRO	Vinit Shukle	23/01/20

Document Distribution

This document will be distributed to:
All Officers and staff

Contents

1. Introduction 4
1.1 Governance 4
1.2 Purpose 4
1.3 Scope 5
1.4 Definitions 6
2. General principles 8
3. Responsibilities and accountability 9
4. Rights of the data subject 11
5. Ensuring information security and confidentiality 12
5.1 Confidentiality of personal information 12
5.2 Security of personal information 13
5.3 Data Protection Impact Assessment (DPIA) 14
5.4 Information sharing 14
5.5 Organisations involved in data sharing 14
5.6 Sharing confidential information without consent 15
5.7 Records management 16
5.8 Deletions and archiving 16
5.9 Training 17
6. Breaches 17
7. Policy Compliance 18
8. Additional policies and guidance 18

1. Introduction

The London Borough of Bromley (LBB) recognises the importance of reliable information and the duty of confidentiality owed to users, employees and third parties with regard to all the ways in which it processes, stores, shares and disposes of information.
//
This policy sets out the obligations of the Council and its employees in relation to the protection of personal data that it holds about or concerning any individual under the General Data Protection Regulation (Regulation (EU) 2016/679).

1.1 Governance

In line with the requirements of ISO27001, the recognised international standard for information security management, this policy will be reviewed no less often than once per year.

The Head of Information Management (or equivalent) has responsibility for ensuring the annual review and that any proposed changes comply with current standards for best practice.

Any variations or rationale for ratifying an un-changed policy must be approved by the Information Governance Sub-group and the Director of Corporate Services.

Please note that the 2019 review has been postponed due to the IT and IM Transformation Programme and that this policy document is still relevant and operative.

1.2 Purpose

The aim of the policy is to ensure that all employees understand their obligations with regard to any information they handle in the course of their work and to provide assurance that the Council has in place the processes, rules and guidelines to ensure that information is dealt with legally, efficiently and effectively.

The Council will establish, implement and maintain procedures to ensure compliance with the requirements of the General Data Protection Regulation, a UK Data Protection Act 2018, other associated legislation and guidance,

contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit.

1.3 Scope

This policy must be followed by all officers who work for or on behalf of the Council including those on temporary contracts, secondments, volunteers, and any third parties acting in partnership with, or on behalf of, the Council.

This policy coversall aspects of information within the Council, including (but not limited to):

- Users' information;
- Employees' information;
- Organisational and business sensitive information;
- Photographic images, digital, text or video recordings including CCTV;
- All information systems purchased, developed and managed by or on behalf of the Council;
- Council information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras.

The processing of all types of information, including but not limited to:

- Obtaining of personal data;
- Obtaining consent for the use of personal data;
- Use of personal data;
- Sharing of personal data;
- Storage and security of personal data;
- Management, arrangement and accuracy of personal data;
- Archiving/disposal of personal data.

The Council recognises the changes introduced to information management as a result of the General Data Protection Regulation 2018 and will work with national bodies and partners to ensure the continuing safe use of information to support its services.

Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed.

If there are conflicting requirements in this policy and national law, please consult with Information Commissioner Office (ICO) for guidance.

This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.4 Definitions

Data Protection Legislation

The General Data Protection Regulation (GDPR) was adopted by the UK in May 2018 The GDPR and the UK Data Protection Act 2018 will replace the previous Directive 95/46/EC on which the Data Protection Act 1998 was based. Its purpose is to protect the rights and freedoms of living individuals and to ensure that personal data is not processed without their knowledge and, wherever possible, that it is processed with their consent.

All organisations must ensure they are fully compliant within the implementation period.

Data Protection Act 2018

The Data Protection Act was announced in the Queen's Speech on 21 June 2017. The Act updates data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR), implementing the EU Law Enforcement Directive, as well as extending data protection laws to areas which are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data.

Personal Data (PD)

Personal Data refers to all items of information in any format from which an individual might be identified or which could be combined with other available information to identify an individual and is information which has a duty of confidence. This includes (but is not limited to):

- Name
- Date of Birth
- Post Code
- Address
- National Insurance Number
- Photographs, digital images etc.
- NHS or Hospital/Practice Number
- Date of Death
- Online identifiers such as IP address and MAC address

Special categories/Sensitive personal data

Certain categories of information are classified as special categories of personal data and additional safeguards are necessary when sharing or disclosing this information in line with guidance and legislation. This includes, but is not limited to:

- Physical and mental health
- Ethnicity and race
- Sexual orientation
- Sex life
- Trade union membership
- Political opinions
- Religious or philosophical beliefs
- Criminal convictions and offences
- Genetic data
- Biometric data

Data subject

The individual who the personal data relates to.

Lawfulness of processing personal data

The legal basis for processing personal data by the Council as a public authority will be one or more of the following conditions under GDPR Article 6:

- Consent for one or more specific purposes;
- Performance of a contract to which the individual concerned is or will be a party of;
- Compliance with the Council's legal obligations;
- Protecting the individual's vital interests, or those of another person;
- Carrying out a task in the public interest or in the exercise of official authority.

Users will also be advised of how the data will be used and can object/withdraw consent if they are not satisfied.

Lawfulness of processing special category of data

Under art. 9 of the GDPR the Council will process Special category personal data under the following conditions:

- Explicit consent
- Employment, social security and social protection
- Vital interests

- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law)

Under art.10 of the GDPR the Council has a lawful basis for processing criminal offence data covering criminal allegations, proceedings or convictions and security measures. This type of data is likely to relate to employment requirements, fraud investigations, safeguarding issues and the vital interests of the data subject or other individuals.

All employees processing special category of data understand their obligations of professional secrecy.

2. General principles

For the Council to be compliant with the General Data Protection Regulation, it must demonstrate consideration of all its principles:

Principle 1: Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner. The Council will inform the data subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in GDPR (lawfulness).

Principle 2: Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The Council will specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The Council will not store any personal data beyond what is strictly required.

Principle 4: Accuracy

Personal data shall be accurate and kept up to date. Each business area will have processes in place for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. The Coucil must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality

Personal data shall be 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. The Council must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability

The Data Controller will be responsible for, and be able to demonstrate compliance. This means the Council must demonstrate that the six Data Protection principles outlined above are met for all personal data for which it is responsible.

3. Responsibilities and accountability

To ensure that the Council meets its responsibilities under the General Data Protection Regulation, it will:

- ensure that Councillors take account of data protection, whilst covering both their roles as ward representatives, and in their broader capacity when acting as representatives of the Council; a separate guidance pack is issued to them;

- appoint or nominate officer/s to deal with data security and access control;

- make all directors responsible for setting a framework within their department, based on this data protection policy, to enable information to be effectively managed and used;

- ensure that all new employees whether permanent, temporary or on work placements, sign a 'confidentiality clause' as part of their contract of employment;

- ensure that all Third parties that have access to personal data have signed a data confidentiality agreement;

- ensure that all employees are given the information governance booklet and are aware of the "do's and don'ts" on data protection as part of the Council's induction process, and have access to appropriate advice when queries or issues arise;

- ensure that job descriptions for managers and supervisors require them at all times to manage and use data for their service area within the Council's data protection policy or other relevant legislation;

- ensure all Information Asset Owners apply proper safeguards and controls proportionate to the level of risk associated with their assets;

- deal with any deliberate misuse of personal information by an employee under the Council's disciplinary procedure.

It is important to note that the Regulations specify that:

- data processors can be held liable for breaches;

- all actual and near missed information breaches should be reported internally to the Principal Information Assurance Officer and to the ICO within 72 hours of becoming known in case of serious breaches of confidentiality.

- the penalty for breach of the Regulations is now capped at a maximum of £18,000,000 or 4% of the turnover of an organisation;

- organisations must employ the privacy by design approach to activities involving personal data. A Data Protection Impact Assessment is required for high privacy risk projects;

- Privacy notices must transparently explain how personal data is used and the rights of the data subject. Organisations outside of the EU are

required to follow the principles of the Regulations if their customers/clients are based within the EU;

- data subjects have the new right to erasure, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period;

- subject access requests must be completed within 30 days and provided free of charge (unless a request is “manifestly unfounded or excessive”).

There are a number of key information governance roles and bodies that the Council needs to have in place as part of its Information Governance Framework, these are:

- Audit Division
- Head of Information Technology
- Head of Information Management
- Principal Information Assurance Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Data Protection Officer
- Information Asset Owners (usually Heads of Service)
- Information Asset Administrators
- Information Coordinator
- Information Champion (role to be confirmed)

4. Rights of the data subject

The Council is committed to support data subject and will facilitate the exercise of individuals’ rights and take measures to promote transparency and accessibility to the information to be disclosed.

Under the UK Data Protection legislation, data subjects have the following rights with regards to their personal information:

Right of access

Data subjects have the right to obtain confirmation as to whether or not personal data concerning them is being prcessed and where that is the case, gain access to the personal data.

Right to rectification
Individuals have the right to ask the Council to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

The right to be forgotten
The right to erase, also known as the 'right to be forgotten', enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to restriction of processing
Individuals have a right to block processing of personal data. When processing is restricted, the Council is permitted to store the personal data, but not further process it.

The right to data portability
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

The right to object
Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and

Rights in relation to automated decision making and profiling
The Council can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

5. Ensuring information security and confidentiality

5.1 Confidentiality of personal information

All activities that relate to personal data, including processing and storing, will have appropriate safeguards and controls to ensure that information is processed in a confidential manner and in compliance with Data Protection laws.

The Council's Conditions of Employment require all staff to respect the confidentiality of personal information revealed to them in their work.

This duty of confidentiality also applies to organisations that provide services under contract or through Service Level Agreements and Information Sharing Agreements. The aim of these documents is to regulate information sharing practices between organisations, to ensure the secure transfer of the data and to identify the legal basis for information sharing.

5.2 Security of personal information

To ensure the security of personal information, the Council employs Data Loss Prevention (DLP) strategies to ensure that users do not send confidential information outside its network.

The Council's systems and data access is role based and operates under the principle of least privilege.

All officers are encouraged to use minimisation, anonymisation and pseudonymisation techniques wherever possible.

Employees have a duty to ensure that personal information, whether held on computer, in case files or in any other manual record, is stored securely.

The System Owner is responsible for the security of personal information held on computer systems. Service Managers are responsible for the security of files and other information held by their teams.

Any breach of security must be reported to line management as soon as possible in line with the Council's Incident Security Reporting Policy.

5.3 Data Protection Impact Assessment (DPIA)

All projects that involve personal data and new processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the Council to address the privacy concerns and risks a technique referred to as a Data Privacy Impact Assessment (DPIA) must be used. The DPIA will:

- identify privacy risks to individuals;
- protect the Council's reputation;
- ensure person identifiable data is being processed safely;
- foresee problems and negotiate solutions.

The GDPR does not require a full GDPR Article 35 Data Protection Impact Assessment (DPIA) to be carried out for every processing operation which may result in risks for the rights and freedoms of individuals. This procedure is only mandatory when the processing of data is likely to result in a high risk to the rights and freedoms of individuals. This is particularly relevant where new technology is being used.

5.4 Information sharing

The Council will ensure that information sharing takes place within a structured and documented process and in line with the ICO Code of Conduct and in accordance with the Council's Information Sharing principles or Information Sharing Agreements.

Any Information Sharing Protocols/agreements that the Council is signed up to need to be followed at all times.

5.5 Organisations involved in data sharing

Managers should ensure that if personal data is processed, all contracts and service level agreements between the Council and external third parties refer to the current Data Protection Act 2018 and GDPR. where necessary, a robust Information Sharing Agreement must be implemented between parties and include at a minimum:

- the purpose of the data sharing initiative;

- details of the organisations that will be involved in the data sharing, including contact details for key members of staff;
- data items to be shared;
- legal basis for processing and sharing
- access and individuals' rights – handling of Subject Access Requests (SARs) and Freedom of Information (FOI) requests;
- assure the quality, accuracy, availability and confidentiality of the data through common technical and organisational security arrangements;
- provision for decommissioning of service or contract/tender including exit strategy identifying retention and destruction of information.

5.6 Sharing confidential information without consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. In this case there must be a legal basis for doing so or an official mandate from a court. When deciding if disclosure of information is permitted, certain considerations and steps need to be taken:

- discuss the sharing requirements with the Head of Service and information Asset Owner if different.
- discuss the request with the appropriate Council officer(s) such as the Information Management team and/or Legal Department.
- disclose only that information which is necessary or prescribed by law.
- ensure recipients are aware that they owe a duty of confidentiality to the information.
- document and justify the decision to release the information.
- take advice in relation to any concerns employees may have about risks of significant harm if information is not disclosed.
- follow any locally agreed Information Sharing Protocols and national guidance.

Requests may be received from other agencies which are related to law enforcement such as:

- the Police or another enforcement agency where appropriate should make a request under Section 43(4) and schedule 2 (2.1) of the Data

Protection Act 2018 (previously section 29 of the Data Protection Act 1998). This request needs to be formally submitted from the law enforcement agency in order for it to be considered by the Council;

- the Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity;
- employees should also take into account the seventh Caldicott principle even if there is a clear legal basis to share. The duty to share information can be as important as the duty to protect patient confidentiality

5.7 Records management

Good record management is a key requirement for the Council to demonstrate accountability for its actions. The Council has a duty to clearly document its decisions and to note down the reasons behind those decisions.

The Council follows its base retention schedule to reflect the lifecycle principles that should be applied to information stored in paper, electronic and other formats.

5.8 Deletions and archiving

There is a clear distinction between deleting data and archiving. GDPR demands that data is not kept for longer than necessary, and this implies deletion, i.e. the destruction of the data.

Archiving on the other hand does not destroy data, it simply removes it from a 'live' system to an alternative storage area (either electronic, e.g. a CD, or actual, e.g. a basement room).

Under GDPR there is a new explicit concept of archiving purposes in the *public interest* to support transparency and legal accountability; archiving needs to secure the permanent availability of evidence and information for a wide range of current and future purposes to enable:

- research and investigation including academic, historical or genealogical research;
- long-term accountability, such as public enquiries and other official investigations;
- the discovery and availability of personal, community and corporate identity, memory and history;

- the establishment and maintenance of rights and obligations of precedent decisions;
- enabling educational use.

5.9 Training

Mandatory Training

Legislation and industry standards require that all employees undergo the information governance training annually.

The Council's Information Governance training will be delivered through the InfoAware portal .

Managers must actively ensure that all staff undertake and complete the mandatory suite of training modules.

Third party Awareness

Third parties acting on the Council's behalf should be aware of and understand their responsibilities towards personal information security and they should receive appropriate training and instruction. Third parties should ensure that only staff working on the Council's behalf get access to personal information and that it is appropriate for them to see this data to undertake their duties.

Monitoring Compliance

Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and reviewed.

6. Breaches

All actual, potential or suspected incidents involving breaches of confidentiality must be reported via the Council's Security Incident Reporting procedure.

All incidents involving users' data should be reported to the Principal Informaiton Assurance Officer. The SIRO should consider whether serious breaches of confidentiality or those involving large numbers of individuals need to be reported to the Information Commissioner Office (ICO).

7. Policy Compliance

All employees are required to meet the requirements of this policy in full and at all times to observe health and safety procedures.

Non-compliance with this policy by any individual working for the Council may result in disciplinary action being taken in accordance with the Council's disciplinary procedure and could lead to dismissal for gross misconduct.

8. Additional policies and guidance

This policy forms part of a suite of Information Management policies which provide further guidance on the Council information standards, data security and working practices which must be adhered to.

Further advice and guidance for staff is available from the Principal Information Assurance Officer.