Hinckley & Bosworth
Borough Council

Hinckley & Bosworth Borough Council
Data Protection Policy

Version number: 1.0
Updated: June 2019
Prepared by: Corporate IG

Contents

1. Introduction

This Data Protection Policy sets out Hinckley and Bosworth Borough Council's approach to handling personal information in accordance with the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) and provides a framework for understanding the requirements of the legislation.
In the course of its everyday business, Hinckley & Bosworth Borough Council ("the Council") collects and process relevant personal data regarding members of staff, volunteers, applicants, contractors and customers as part of its operation and to take all reasonable steps to do so in accordance with this Policy. This policy applies in all cases where the Council is the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used.

The policy provides an overview of the main obligations for Officers and Elected members in dealing with personal information so they can comply with the transparency, accountability, data processing, and other principles established under this legislation and the exercise of the individual rights.

2. General Statement of the Council's Duties and Scope

The Council is committed through its policy, procedures and guidelines and the Data Protection Officer to ensure that its will:

- Comply with both the law and good practice
- Respects individual rights
- Be open and honest with individuals whose data is held

At the heart of the Act is the need to protect personal information (otherwise known as personal data) and put additional protection in place for the special categories of sensitive personal data.

3. Definitions

Personal Data means any data that is considered as Personal Data under the Data Protection Regulation, specifically information relating to an identified or identifiable natural person. 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.

A Data Controller is any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

A Data Processor is any natural or legal person, public authority, agency or other body which processes Personal Data on behalf of a Data Controller.

A Data Subject is any identified or identifiable natural person from whom Personal Data is collected.

Processing or Processed means every operation or set of operations which is performed with regard to Personal Data , including without limitation the collection,

recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combining, linking to other data, blocking, erasure or destruction of Personal Data .

General Data Protection Regulation or GDPR is the UK Data Protection Act 2018 (DPA) and EU General Data Protection Regulation 2018 (GDPR)

Automated decision-making is a decision made without human intervention solely by algorithms, computer analysis or other automatic means.

Personal Data Breach or Breach means any suspected or actual security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

4. Data Protection Principles

The GDPR places responsibilities on both the Council as an organisation, but also on any individuals handling Personal Data. It is recognised that in the course of their authorised duties most elected members and staff will need to handle and/or process personal information. As a consequence, all elected members and staff should be aware of the data protection principles, which must be complied with at all times.

The GDPR sets out seven key principles:

4.1 Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. The Council, elected members and staff must tell the Data Subject what processing will occur. This is known as “transparency”, the processing must match the description given to the Data Subject in order to meet the “fairness” requirement, and it must be for one of the purposes specified in the applicable legislation “lawfulness”.

4.2 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, elected members and staff must specify exactly what the Personal Data collected will be used for and limit the use of the data to the reason for it being collected.

4.3 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, elected members and staff must not store any Personal Data beyond what is strictly required.

4.4 Principle 4: Accuracy

Personal Data shall be accurate and kept up to date. The Council, elected members and staff must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

4.5 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 Council, elected members and staff must, wherever possible, store Personal Data in a way that limits or prevents identification of the data subject.

4.6 Principle 6: Integrity & Confidentiality (security)

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, elected members and staff must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

4.7 Principle 7: Accountability

Underpinning the above is the principle of accountability. The Council shall be responsible for, and be able to demonstrate, compliance. All elected members and staff must demonstrate that the data protection principles, outlined above, are met for all Personal Data for which they are responsible.

The principles were been adopted by the Council on 25 May 2018 in order to govern its collection, use, retention, transfer, disclosure and disposal of Personal Data .

4.8 Sharing Data - interpretation of the principles

There is an increasing demand and expectation that Personal Data will be shared with other public bodies. This often improves efficiency and service delivery within the Council. In addition there is also a requirement to share information with other public bodies for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty or an imposition of a similar nature.

The Information Commissioner has offered the following advice on sharing data between different local authority departments or services, and other public bodies: -

- The Information Commissioner's advice is that the first principle must be satisfied, particularly 'Personal Data shall be processed fairly and lawfully' but local authorities can process data if carrying out of a task in the public interest or in the exercise of official authority. The Information Commissioner does however state that to ensure the fair processing, the data subject should be made aware of any 'non- obvious' purposes for which the information may be used or disclosed.

- Equally the Information Commissioner is concerned that in any data sharing, the second principle is properly considered. If data has been collected for a specified purpose, the Council should not use that data for another purpose, unless the

data subject has given consent, or there is another lawful reason allowing for the data to be used in the proposed manner.

- It will also be necessary to consider the legislation that supports any Council activities that require data sharing. The legal considerations for data sharing are both complex and difficult. There is a requirement to interpret and exercise judgement on the Principles of the Act in light of the particular circumstances where the information is to be shared with another public body. If service managers have particular issues in this area, they should contact the Council's Data Protection Officer.

The Council will only share Personal Data with other organisations and third parties where the sharing is necessary to achieve a clear objective and it is fair and lawful to do so.

Routine sharing of data between organisations for an agreed lawful purpose will be undertaken in accordance legislation or with a signed and formal Information Sharing Agreement.

5. Safeguarding

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 provide a number of important safeguards and rights for Personal Data held about living individuals (natural persons).

These safeguards apply to:

- Personal Data held in any organised filing system - the data can be held electronically or automatically processed by a computer or in manually maintained systems, for example case files, card indexes etc. The conditions of the GDPR apply if specific information about an individual is readily accessible.
- Personal Data means information which relates to an identified or identifiable living individual, including any opinions about them.
- Processing Personal Data, including obtaining, recording, holding, organising, retrieving, using, disclosing and destroying information.

6. Responsibilities of Elected Members and officers

6.1 Elected Members

When Members process Personal Data whilst acting as a representative of residents of their electoral ward and /or whilst representing a political party, they do so independently from the Council's registration with the Information Commissioner. However, where an Elected Member has access to and processes personal information on behalf of the Council, the Member does so under the Council's registration and must comply with this policy.

6.2 Chief Executive and Directors

The Chief Executive and Directors are responsible for implementing safe and sound data protection procedures within their services and the operation of those services and ensuring the proper security of information held. Directors should have regard to The Data Protection Policy, the Information Governance Framework and the

Acceptable IT Use Policy when formulating any policies or procedures which make use of Personal Data.

6.3 Data Protection Officer

The Council's Constitution, through its scheme of delegation, ensures that a named individual has specific operational responsibility for data protection matters corporately. That person is The Data Protection Officer. The Data Protection Officer shall be accountable for

- Reviewing and making recommendations for Data Protection and related policies
- Advising staff on Data Protection issues and the rules to ensure compliance with data protection laws with the assistance of legal Services as required. The Data Protection Officer shall report to the Chief Executive.

64 Information Governance Officer

Within the Corporate Team there will be an Information Governance Officer with specific responsibility for data protection compliance and for advising and training on data protection matters. The Information Governance Officer shall report to the Data Protection Officer.

6.5 Senior Information Risk owner

The Senior Information Risk owner (SIRO) has overall strategic responsibility for governance in relation to data protection risk. The SIRO:

* Acts as advocate for information risk at the Corporate Leadership Team.
* Oversees the reporting and management of information incidents.

The SIRO will assist the organisation to consider the information risks associated with its business goals and how those risks will be managed.

The Senior Information Risk Owner for the Council is Julie Kenny.

6.6 Information Security Manager

The Information Security Manager is responsible for creating, implementing and maintaining the Council's security policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation.

6.7 All Staff

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection principles and that information held by the Council is accurate and up-to-date.

All new staff will receive basic training on the data protection as part of their induction. Managers should ensure all staff for whom the manager is responsible receive appropriate training on the Data Protection legislation, on the application of this Policy and on their individual responsibilities.

7. Security of data

7.1 Information access

All staff are responsible for ensuring that Personal Data which they use or process is kept securely and is not disclosed to any unauthorised person or organisation.

Access to Personal Data should only be given to those who have and can show a need for access to the data for the purpose of their duties.

All staff and Elected Members have a responsibility to ensure that any Personal Data they see or hear is not disclosed to third parties unless there is clear and specific authority to do so. This includes Personal Data and information extracted from such data, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or by allowing it to be read on a computer screen.

7.2 Acceptable IT Use

The Data Protection Officer shall ensure that an Acceptable IT Use Policy is in place that covers all aspects of activity and conduct so as to ensure compliance with the Council's obligations in relation to electronically held information and that such a Policy is kept up to date and drawn to the attention of all staff.

All staff and Elected Members must read and comply with the Acceptable IT Use Policy, which must be signed as read by all staff before access to information containing Personal Data is permitted. The Acceptable IT Use Policy is permanently accessible on the Council's intranet.

7.3 Hard copy data

Personal Data should not be left where it can be accessed by persons not authorised to see it or have access to it.

Procedures shall be put in place by the Director responsible for Council buildings and facilities, relating to access to the Council's buildings so as to ensure the security of data. Procedures in regards to access to buildings and particular parts of buildings should be communicated to all staff and members and adhered to by all.

7.4 Data destruction

Personal Data which is no longer required must be destroyed appropriately, for example, by shredding or, in the case of computer records, secure deletion. Computers must have all personal information securely deleted using the appropriate software tools. Personal Data must be destroyed in accordance with the Council's retention schedule.

7.5 Working from home

Staff working from home must have particular regard to the need to ensure compliance with this policy, the Flexible Working Policy and the Acceptable IT Use Policy. The security and proper processing of data outside offices and usual places of work, and whilst travelling, must be ensured.

7.6 Data breaches

Personal Data security breaches will be detected, reported and investigated in accordance with the data breach procedure. All staff must be aware of and follow the data breach procedure available on the Council's intranet and included in induction training for all new members of staff.

Serious breaches where there is a high risk to the rights of the individual must be reported to the Information Commissioner's Office by the Data Protection Officer within 72 hours.

Staff and Elected Members must therefore report Personal Data Breaches or potential breaches as soon as possible to the Information Governance Officer. The sooner action is taken; the greater the opportunity there is to limit any potential damage which might be caused by the incident.

The Data Protection Officer will decide whether it is necessary to report the Personal Data Breach to either the Information Commissioner's Office, to the affected Data Subjects, or any involved third parties.

8 Data subjects' rights

The GDPR contains data subject rights that the Council must comply with. The Council must respond to these requests within four weeks. The rights are as follows:-

8.1 Right of access by the data subjects

Individuals have the right to request to see or receive copies of any information the Council holds about them, and in certain circumstances to have that data provided in a structured, commonly used and machine readable format. It is a personal criminal offence for any Elected Member of member of staff employed by the Council to delete relevant Personal Data after a subject access request has been received.

8.2 Right to rectification

Individuals have the right to have inaccurate Personal Data rectified. An individual may also be able to have incomplete Personal Data completed. The Data Protection Officer is responsible for determining whether Personal Data is inaccurate before any rectification can be made to personal information held by the Council.

8.3 Right to erasure ('right to be forgotten')

Individuals have the right to have Personal Data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. The Data Protection Officer is responsible for determining whether personal information held by the Council can be legally removed.

8.4 Right to restriction of processing

Individuals have the right to request the restriction or suppression of their Personal Data. This means that an individual can limit the way that an organisation uses their information. This is an alternative to requesting the erasure of their data. The right to

restriction is not an absolute right and only applies in certain circumstances. The Data Protection Officer is responsible for determining whether personal information held by the Council can be legally restricted.

8.5 Right to data portability

The right to data portability gives individuals the right to receive Personal Data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

8.6 Right to object

This gives individuals the right to object to the processing of their Personal Data. This effectively allows individuals to ask the Council to stop processing their Personal Data.

The right to object only applies in certain circumstances. Whether it applies depends on the purposes for processing and the lawful basis for processing. The Data Protection Officer is responsible for determining whether an objection is valid before any further processing can be conducted using the personal information in question.

8.7 Automated individual decision-making, including profiling

The GDPR restricts the Council from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. If an individual requests that an automated decision be reviewed by a natural person, this is a request under Article 22 of the GDPR and must be relayed to the Data Protection Officer.

9. Conditions and Lawfulness of Processing Information

9.1 Lawfulness of processing

In order to meet the ‘lawfulness’ requirement, processing Personal Data must meet at least one the following conditions:

- The data subject has given consent.
- The processing is required due to a contract.
- It is necessary due to a legal obligation.
- It is necessary to protect someone’s vital interests (i.e. life or death situation).
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- It is necessary for the legitimate interests of the Council or a third party.

9.2 Processing of special categories of Personal Data

Special category data is Personal Data which is deemed more sensitive under GDPR, and so needs more protection. This covers information concerning racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health and sex life and sexual orientation.

For special categories of Personal Data, at least one of the following conditions must also be met:

- The data subject has given explicit consent.
- The processing is necessary for the purposes of employment, social security and social protection law.
- The processing is necessary to protect someone's vital interests.
- The processing is carried out by a not-for-profit body.
- The processing is manifestly made public by the data subject
- The processing is necessary for legal claims
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
- The processing is necessary for public health
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards.

10. Accountability and governance

10.1 Data Subject Notification (Privacy Notices)

Each Service Area will provide data subjects with information as to the purpose of the processing of their Personal Data, this is known as a Privacy Notice.

A mandatory privacy notice should be provided whenever the council is collecting and processing customer Personal Data.

Privacy Notices explain to individual persons the purpose for collecting Personal Data and should contain the following information:

- The name and contact details of the Controller and Data Protection Officer
- The purpose and legal basis of processing the data.
- Retention period for the data collected
- The identity of those with whom the data is shared.
- The rights of the individual as in part 7 of this policy.
- The existence of automated decision-making, including profiling

The Council's website will contain an over-arching top level corporate privacy notice which will cover processing activities and information rights. In addition to the online 'Privacy Notice' an online 'Cookie Notice' will be available, fulfilling the requirements of applicable law.

Any future changes to the corporate privacy, cookie and task based policies and notices, should be approved by the Data Protection Officer and or the Information Governance Officer, prior to online publication.

All privacy notices should be available in hard copy upon request.

10.2 Data protection by design and default

To ensure that all Data Protection requirements are identified and addressed when designing new systems and processes, or when reviewing or expanding existing systems or processes, an approval process must be undertaken before continuing. This process is called a Data Privacy Impact Assessment (DPIA).

The DPIA process helps identify and minimise the data protection risks of a project. A DPIA must be undertaken where processing information is likely to result in a high risk to individuals, but it is good practice for assessments to be carried out for any other major projects which require the processing of Personal Data.
A DPIA must:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks

Where applicable, the Information Technology (ICT) team will cooperate with the Data Protection Officer and Information Governance Officer to assess the impact of any new technology uses on the security of Personal Data.

10.3 Records Management

Good records management practice plays a pivotal role in ensuring that the Council is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet its legal requirements.

It is necessary to ensure that robust records management practices are in place which are understood and implemented by all staff dealing with records within the Council.

It is the responsibility of all staff to ensure that they are familiar with the policies, procedures and schedules relating to records management within the Council, including the Records Management Policy. All records should be retained and disposed of in accordance with the Council's retention schedules.

10.4 Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by services/departments in relation to this policy, the Council will carry out regular data audits of service areas. Each audit will, as a minimum, assess compliance with Policy in relation to the protection of Personal Data, including:

- The assignment of responsibilities.
- Raising awareness.
- Training of Employees.
- The effectiveness of Data Protection related operational practices.
- Personal Data transfers.
- Data Breach management.
- Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.

- The currency of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.

The audit will include the development of any remedial action plans and will be implemented by the service manager of the affected service area.

11. Risks

The risks of not ensuring adequate data protection compliance could be; incurring of monetary penalties if a breach of the Data Protection Act occurs; complaints from the community if their privacy rights are violated and loss of reputation through a lack of trust by the community in handling confidential information.

The Corporate risk register monitors the requirement to ensure all staff are fully aware and trained in GDPR compliance. All service areas have risk registers which will include any specific data protection risks and actions taken to mitigate them.

The use of a customer's information should always be considered from their perspective and whether the use will be within their expectations.

12. Review

The Council will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, the Council will not process Personal Data unless the requirements of this policy are met. The Information Governance Officer is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

13. **Complaints**

The first point of contact for Data Protection complaints will be required to be addressed to the data Protection Officer and sent to:-
Hinckley & Bosworth Borough Council,
Hinckley Hub,
Rugby Road, Hinckley,
Leicestershire,
LE10 0FR.

Under DPA the data subject has a specific right to complain to the ICO if they feel the Council is not processing their data lawfully. Complaints can be sent to:

Customer contact
Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow
Cheshire
SK9 5AF.

Alternatively visit their website- www.ico.gov.uk or contact them on 03031231113.