****

**HARBOROUGH DISTRICT COUNCIL**

**INFORMATION GOVERNANCE POLICY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Purpose/Change | Author | Date |
| V1.1 | Original final text | R Ellis | September 2017 |
| V1.2 | Interim update | S Done | July 2019 |
|  |  |  |  |
|  |  |  |  |

1. Introduction

Information is a key organisational asset and is vital to effective decision making, service planning, delivery and performance management. It is of paramount importance that the information the Council holds is efficiently managed and that appropriate standards, policies and procedures provide a robust governance framework.

1. Purpose

The purpose of the Information Governance Policy is to provide an over-arching framework which will set out how the Council manages its information assets with the aim of ensuring that Harborough District Council:-

* Meets its legal obligations for the effective management of information
* Recognises the key enabling role of information in delivering council objectives
* Ensures that information is treated as a valuable asset
* Ensures that sensitive personal data is held and processed securely

1. Objectives

The objective is to ensure that the Council:-

* Holds information securely and confidentially
* Obtains information fairly and efficiently
* Records information accurately and reliably
* Uses information effectively and ethically
* Shares information appropriately and lawfully
* Has appropriate information available to support service improvement, transparency and openness, public accountability and open data initiatives.

1. Scope

The policy applies to:

* All information held and used by Harborough District Council. Information and data takes many forms and includes information and data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes, disks or other electronic media and spoken in conversation or over the telephone
* All information systems, manual or electronic, operated or managed by Harborough District Council

1. Legal Framework

There are a number of legal obligations placed upon the council governing the use and security of the information it holds which are supported by a variety of standards and best practice guides.

* Data Protection Act 2018
* General Data Protection Regulations 2016
* Human Rights Act 1998
* Freedom of Information Act 2000 (as amended by the Protection of Freedoms Act 2012)
* Regulation of Investigatory Powers Act 2000
* Investigatory Powers Act 2016
* Environmental Information Regulations 2004
* Re-use of Public Sector Information Regulations 2005
* Infrastructure for Spatial Information in the European Community (INSPIRE ) Regulations 2009
* Regulation of Investigatory Powers Act 2000
* Local Audit and Accountability Act 2014 (sections 25 and 26)
* Local Government Transparency Code 2015
* Localism Act 2011

1. Information Management

The Council has a framework of policies and operational practices to ensure that it complies with the Information Governance areas already referred to above covering the following areas:

• Freedom of Information and Openness.

• Data Protection and Confidentiality.

• Records Management (including copyright law).

• Information Security and Risk Management.

• Information Quality.

* 1. Freedom of Information and Openness

The Council’s duty to provide public access to information it holds is primarily governed by the provisions of the Freedom of Information Act 2000 and Environmental Information Regulations 2004. In general terms the Council has a duty to provide information on request within a period of 20 working days unless a relevant exemption (Freedom of Information) or exception (Environmental Information) exists. Sensitive personal data (as defined by the Data Protection legislation) is excluded, although consideration must be given to publication with the sensitive personal data redacted (removed) if it is possible and appropriate to do so.

The person making a request does not have to state that they are making a request under the legislation and it is a duty of the Council to accept the request and to apply the provisions of the relevant legislation to it.

The Council is required to publish a Publication Scheme which lists information which is already published and available and how it can be accessed.

In most circumstances the Council cannot charge for compiling information to respond to an information request.

If the Council fails to meet the timeframes for providing information laid down in the legislation or claims one of the exemptions the person submitting the request has the option of appealing to the Information Commissioner, who will review the Council’s handling of the request,

[Relevant Policies/Guidance](http://www.harborough.gov.uk/intranet/directory_record/12078/information_and_data_management):

* Information Requests Procedure
* Publication Scheme
* Freedom of Information Exemptions Guidance
* Environmental Information Regulations Exceptions Guidance
* Information Commissioner’s Website
  1. Data Protection and Confidentiality

The Data Protection legislation places responsibilities on both the organisation and those individuals handling the 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 consequence, all elected members and staff are required to comply with the six data protection principles:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; and

f) 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.

The Council has guidelines and policies in place to assist corporate compliance with the six data protection principles.

In order to comply with the above, for the processing of personal data to take place, at least one of the following MUST apply:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. **(This cannot apply if you are a public authority processing data to perform your official tasks.)**

[Relevant Policies/Guidance:](http://www.harborough.gov.uk/intranet/directory_record/12078/information_and_data_management)

* Data Protection Guidelines
* Clear Desk Policy
* Data Protection and Confidentiality in the Workplace
* Data Protection Act Process Flow
* Data Loss Procedure
* Data Loss Report Form
* Data Protection Act – ICO Guidance on the use of Privacy Notices
* Information Sharing Protocol (Includes template Information Sharing Agreement )
* Data Protection Act - ICO Code of Practice on Privacy Impact Assessments
* HDC Template on Data Protection Impact Assessments (DPIA’s)
  1. Records Management (including copyright law)

In the course of its business the council creates a vast amount of information in both electronic and paper form. Legislation dictates that certain information is retained either in perpetuity or for a defined period of time before destruction. The Document Retention Policy sets out the Council’s agreed retention periods for various categories of information. Files and related information must be kept in accordance with the policy and no information should be disposed of without a record being kept of the data sets subject of destruction, the date of destruction and which section of the Document Retention Policy the destruction is authorised.

[Relevant Policies/Guidance:](http://www.harborough.gov.uk/intranet/directory_record/12078/information_and_data_management)

* Document Retention Policy
* Disposal Log
  1. Information Security and Risk Management

The Council manages security of electronic data through application of a number of policies and procedures aimed at ensuring that staff and councillors are aware of their responsibilities and appropriate operational requirements which must be observed.

Risk of data loss is managed through regular system backups and through the ICT disaster recovery plan. In a business recovery scenario the plans maintained by each service area and feeding into the Corporate Business Continuity Plan inform the order of recovery of ICT systems.

The ICT Security Policy covers use of laptops and other portable ICT devices within and outside of The Symington Building.

Service managers are also required to have regard to information they may hold in a form which is not electronic. The Data Protection principles and operational requirements set out in Section 6.2 apply to both electronic and paper based records and sensitive paper based records must be protected by adequate security measures whilst in use within the office or if taken off-site as required by the Flexible Working Policy.

[Relevant Policies/Guidance:](http://www.harborough.gov.uk/intranet/directory_record/12079/governance)

* ICT Security Policy
* Email Usage Policy
* Email Archiving Procedure
* GCSx Personal Commitment Statement
* Internet Usage Policy
* Removable Media Policy
* Flexible Working Policy
  1. Information Quality

Information is a key organisational asset and it is therefore imperative that information obtained, produced and held by the council is of the highest quality. High quality information is dependant on high quality data (garbage in, garbage out). The Data Quality Strategy sets out the Council’s approach to data quality.

Data quality is the responsibility of every employee who enters, extracts or analyses data from any of the Council’s information systems and records. Every employee needs to be aware of his or her responsibilities for quality of data.

Relevant Policies/Guidance:

* [Data Quality Strategy](file:///\\hdc-fs2\Public\Data%20Quality\Data%20Quality%20Strategy%202015%20Edition)
* [Performance Management Framework and KPI Definition Documents](file:///\\HDC-FS2\Departmental\Political\incoming\Executive\2016\11%20January%202016%20(Budget)\Performance%20Management%20Framework)
* [Risk and Opportunity Management Framework](file:///\\HDC-FS2\Departmental\Political\incoming\Executive\2016\11%20January%202016%20(Budget)\Risk%20and%20Opportunity%20Management%20Framework)

1. Elected Members
   1. Councillors must ensure that Data Protection legislation and policies are complied with whatever role they may exercise.
   2. If a Councillor is processing data for their ward member purposes they must register with the Information Commission as a data controller as well as ensure compliance with the principles of the Data Protection legislation.
2. Information Sharing
   1. The Council will require its partners and agents through contractual terms, partnership agreements and information sharing agreements to comply with the law when providing services to the Council and when sharing data with the Council.
   2. Service Managers responsible for procurement of services must ensure that privacy impact assessments are carried out, potential bidders are compliant with data protection requirements and the necessary Data Processing Agreements are put in place when contracts are awarded.
   3. Managers responsible for services which share personal data with outside partners and agencies must ensure that a written Information Sharing Agreement is in place. The Information Sharing Agreement must be agreed by the Legal Team and Information and Complaints Officer, who will record a copy centrally for monitoring and compliance purposes.

8.4 Any Information Sharing Agreement must be signed by a Corporate Director.

1. Training and Compliance

9.1 The Council recognises the need to make the contents of this Policy known and ensure compliance by every employee.

9.2 All staff will be mandatorily trained in basic information access and Data Protection principles and made aware of this policy and of relevant guidance and publications which are available. Freedom of Information and Data Protection awareness will be included in both the corporate induction course through the Council’s e-learning package, Learning Matters. Face to face training updates for staff will also be provided annually or as demand requires. The Information Governance Officer will notify staff of changes to Freedom of Information and Data Protection legislation, how these changes will affect them, when they will occur and what is needed to stay within the law.

9.3 Training in Freedom of Information, Environmental Information and Data Protection will be provided for all councillors as part of mandatory councillor training and on an ad hoc basis as demand requires.

9.4 The Council must notify the Information Commissioner’s Office annually which classes of data it intends to process. An internal review of notification requirements will be undertaken annually and the Information Commissioner informed of any changes required in notification.

9.5 Harborough District Council expects all employees to comply fully with this policy and the individual policies and guidance notes referenced herein. Disciplinary action may be taken against any Council employee who knowingly breaches any instructions contained in, or following from this policy.

9.6 Individual employees are affected in the same way as the Council as a whole. Anyone contravening the Freedom of Information Act 2000 and/or Data Protection legislation could be held personally liable and face court proceedings for certain offences which may result in a fine and / or a criminal record.

10.0 Information Officer Designations

* HDC identifies the current Information and Complaints Officer as the new Information Governance Officer and designated Data Protection Officer.
* Current details being:

**Stuart Done** | **Information Governance Officer**

Harborough District Council

tel: 01858 821164 | mob: 07766 206066 | email: [s.done@harborough.gov.uk](mailto:s.done@harborough.gov.uk)

Secure Mail: [s.done@harborough.gcsx.gov.uk](mailto:s.done@harborough.gcsx.gov.uk)

Or:

Email: [FOI@harborough.gov.uk](mailto:FOI@harborough.gov.uk)

* Senior Information Risk Officer (SIRO) Corporate Director: Beverley Jolly.