Data Protection Policy

Document Control Information	
Document Title	Data Protection Policy
Version	3.0
Status	Published
Author	Peter Richmond
Job Title	Divisional Manager, Service Improvement,
Department	ICT Services
Publication Date	3rd December 2018
Approved by	Information Governance Group/ICT Strategy Board
Next review date	December 2019
Distribution	All staff as referred to in the coverage section of this policy
Classification	Unclassified
Any comments on the Policy should be given to the Divisional Manager, Service Improvement Division	

Version Control Information	Date	Comments
Policy Published Version 2.0	10th May 2018	
Policy Reviewed Version 3.0	3rd December 2018	Added section 3.3

Contents

1. INTRODUCTION

Halton Borough Council recognises its responsibility to comply with the General Data Protection Regulation (GDPR) and all other relevant legislation and regulations. GDPR regulates the use of personal data, this does not have to be sensitive data, it can be as little as a name and address.

2. GENERAL DATA PROTECTION REGULATION (GDPR)

The regulation sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how information can be collected, stored, processed and used. It applies to anyone holding information about people electronically or on paper.

The regulation says that the information provided to people about how we process their personal data must be concise, transparent, intelligible and easily accessible, written in clear and plain language, particularly if addressed to a child and free of charge.

Halton Borough Council has procedures in place to ensure that it complies with data protection legislation when holding personal information.

When dealing with personal data Halton Borough Council will ensure the data protection principles set out under the GDPR are adhered to; that personal data shall be:

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."

3. DEFINITION OF PERSONAL AND SENSITIVE DATA

GDPR provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

3.1 Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.2 Sensitive personal data

The GDPR refers to Sensitive personal data as 'special categories of personal data'; 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
Criminal proceedings or convictions
Genetic data and biometric data where processed to uniquely identify an individual

3.3 Processing of personal and sensitive data

The Council considers that all personal data should be processed to the same standard and this is the standard applicable to sensitive processing. Consequently, in this policy all references to the controller's procedures for securing compliance with the data protection principles apply to sensitive processing as well as non-sensitive processing and all of the controller's policies as regards the retention and erasure of personal data shall apply equally (subject to section 42(3) Data Protection Act 2018) to sensitive processing. The controller considers that this policy also constitutes an appropriate policy document in relation to sensitive processing as defined in section 42 Data Protection Act 2018.

3.4 Personal data and safeguarding

Where, in the judgement of a practitioner, an individual is thought to be at risk, the practitioner must not seek the consent of any person who, if they knew that their personal data was being shared, might put the individual at further risk.

Practitioners who record or pass on personal data without seeking consent, as set out above, must record this against the relevant social care record.

4. COVERAGE

This Policy applies to all Halton Borough Council employees, agency workers, external contractors,

casual workers, volunteers, employees from other organisations using Halton Borough Council equipment, elected members and those working on secondment (referred to herein as "staff").

This policy applies to all personal data throughout the whole lifecycle held both on paper and by electronic means.

5. POLICY STATEMENT

Halton Borough Council needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include members of the public, current, past and prospective employees, clients and customers and suppliers. In addition the Council may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Halton Borough Council regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the Council and those with whom it carries out business. The Council therefore fully endorses and aims to adhere to the requirements of data protection legislation.

6. COMPLIANCE WITH GDPR

In order to meet the requirements of data protection legislation, Halton Borough Council will, through appropriate application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information.
- Identify the lawful basis for any personal data we process and document it.
- Demonstrate compliance with the accountability principle by implementing appropriate technical and organisational measures, including maintaining an Information Asset Register, data protection impact assessments, staff training and internal data protection policies.
- Meet its legal obligations to specify the purposes for which information is used; including specific requirements that must be met to ensure fair and lawful sharing of personal data both internally and externally. Secure facilities are available for sharing information.
- Ensure that the Council's Notification to the Information Commissioner's Office remains up to date and accurate.
- Collect and process appropriate information, and only to the extent that is needed to fulfil operational needs or to comply with any legal requirement.
- Ensure compliance with GDPR through written contracts with data processors
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held according to the Records Retention Policy and Schedule.
- Ensure that the rights of people about whom information is held, are able to be fully exercised under the regulation. These include the right to be informed that processing is undertaken, the right of access to personal information, the right to prevent processing in certain circumstances and the right to correct rectify, block or erase information which is regarded as wrong information, the right to object in certain circumstances.
- Ensure compliance with Halton Borough Council's Information Security, Acceptable Use and Removable Media Polices to safeguard personal information.
- Ensure that information is not transferred abroad without suitable safeguards.
- Ensure that the Council has breach detection, investigation and internal reporting procedures in place.

- In line with the above, ensure that all staff are aware of requirements of the Council's Information Governance Handbook and how to report and manage personal data breaches.

7. STAFF ROLES AND RESPONSIBILITIES

7.1 Data Protection Officer (Service Improvement Divisional Manager)

Halton Borough Council has appointed a Data Protection Officer – Peter Richmond, Divisional Manager Service Improvement and Governance.

The Data Protection Officer is responsible for gathering and disseminating information and issues relating to Data Protection and for leading on formulating policy and best practice.

The Data Protection Officer produces bi-annual reports for the Senior Information Risk Owner (SIRO).

7.2 Information Governance Team and Security and Policy Team

The Information Governance Team and the Security and Policy Team will work closely with the Data Protection Officer to carry out the day to day workings of Data Protection compliance.

7.3 Information Governance Group

The Information Governance Group will be made aware of all data protection tasks and will help to coordinate Data Protection Compliance.

7.4 Halton Borough Council Staff

Although there are dedicated roles for Data Protection it is the responsibility of all staff acting on behalf of the Council to safeguard personal data in their care. Therefore staff members are required to be aware of the provisions of the legislation, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of the Authority.

Line Managers are responsible for Data Protection compliance within their operational area. Heads of Service must identify all computer and manual systems that contain personal data and ensure this information is included in the corporate Information Asset Register. This will ensure that all necessary actions are being undertaken to comply with data protection legislation.

Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken or criminal prosecution. If a staff member suspects, or witnesses a data protection breach they should inform their Line Manager and the Divisional Manager Service Improvement and Governance immediately.

Under GDPR legal liability for the safeguarding of personal data falls both to the organisation and through its employment and other contractual arrangements individually to its staff members. Prosecutions and other enforcement action have been undertaken under the regulation and through disciplinary processes.

8. ACCESSIBILTY

If the Data Protection Policy is required in different formats such as large print, audio tape and Braille please go the following link for information:
http://intranet/Pages/Interpretation%20and%20Translation-Guidance.aspx

9. SUPPORTING DOCUMENTATION

This policy should be read in conjunction with -

Information Security Policy
Acceptable Use Policy
Information Governance Handbook
Subject Access Request Policy
Records Management Policy
Records Retention Policy
Information Sharing Policy
Disciplinary Procedure
Removable Media Policy
Information Security Leaflet

In the event of any conflict with the Constitution or the above procedures, then the Constitution prevails.

December 2018